DIGITALSIGN - CERTIFICADORA DIGITAL, SA.

DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO

VERSÃO 3.7 – 15/06/2021

HISTÓRICO DE VERSÕES

Data	*Edição n.º*	*Conteúdo*
20/07/2009	1.0	Redação Inicial
21/06/2010	1.1	Revisão
07/01/2011	1.2	Alteração de denominação
22/02/2012	1.3	Alteração de membros e atribuições do Grupo de Gestão
28/03/2013	2.0	Revisão e inclusão de perfil de Certificado de Validação Cronológica
23/10/2013	2.1	Revisão
25/03/2015	2.2	Revisão
01/07/2016	3.0	Adaptação ao Regulamento (EU) n.º 910/2014
18/10/2016	3.1	Revisão
20/07/2017	3.2	Revisão para inclusão da Solução de Assinatura Remota
21/12/2017	3.3	Revisão
29/01/2018	3.4	Revisão
19/09/2018	3.5	Revisão
20/09/2019	3.6	Revisão
15/06/2021	3.7	Revisão

AVISO LEGAL

CONTEÚDO

1. Introdução 10
1.1. Contextualização 11
1.2. Designação e Identificação do Documento 12
1.3. Participantes na PKI 12
1.3.1. Entidades Certificadoras 12
1.3.2. Entidades de Registo 12
1.3.3. Titulares dos Certificados 13
1.3.4. Partes Confiantes 13
1.3.5. Outros Participantes 13
1.4. Utilização do Certificado 13
1.4.1. Utilização Adequada do Certificado 13
1.4.2. Utilização Não Autorizada 14
1.5. Gestão de Políticas 14
1.5.1. Entidade Responsável pela Gestão do Documento 14
1.5.2. Contactos 14
1.5.3. Determinação de Conformidade 14
1.5.4. Procedimentos de Aprovação 15
1.6. Acrónimos e Definições 15
2. Responsabilidades de Publicação e Repositórios 16
2.1. Repositórios 16
2.2. Publicação da Informação dos Certificados 16
2.3. Periodicidade de Publicação 16
2.4. Controlo de Acessos aos Repositórios 17
3. Identificação e Autenticação 18
3.1. Atribuição de Nomes 18
3.1.1. Tipos de Nomes 18
3.1.2. Necessidade de Nomes Significativos 18
3.1.3. Anonimato ou Pseudónimos dos Titulares 19
3.1.4. Regras para Interpretação dos Vários Formatos de Nomes 19
3.1.5. Singularidade dos Nomes 19
3.1.6. Reconhecimento, Autenticação e função das Marcas Registadas 19
3.2. Validação Inicial de Identidade 19
3.2.1. Método para Prova de Posse da Chave Privada 20
3.2.2. Autenticação de Identidade de uma Pessoa Coletiva 20
3.2.3. Autenticação de Identidade de uma Pessoa Singular 20
3.2.4. Informação do Titular não Verificada 20
3.2.5. Validação de Autoridade 21

3.2.6. Critérios para Interoperabilidade 21
3.3. Identificação e Autenticação para Pedido de Renovação de Chaves 21
3.3.1. Identificação e Autenticação para Renovação de Chaves, de Rotina 21
3.3.2. Identificação e Autenticação para Renovação de Chaves, após Revogação 21
3.4. Identificação e Autenticação para Pedido de Revogação 22
4. Requisitos Operacionais 23
4.1. Pedido de Certificado 23
4.1.1. Quem pode subscrever um Pedido de Certificado 23
4.1.2. Processo de Inscrição e Responsabilidades 23
4.2. Processamento do Pedido de Certificado 24
4.2.1. Funções de Identificação e Autenticação 24
4.2.2. Aprovação ou Recusa de Pedidos de Certificado 24
4.2.3. Prazo para Processamento do Pedido de Certificado 24
4.3. Emissão de Certificado 25
4.3.1. Procedimentos para Emissão de Certificado 25
4.3.2. Notificação de Emissão de Certificado ao Titular 25
4.4. Aceitação do Certificado 25
4.4.1. Procedimentos para Aceitação do Certificado 25
4.4.2. Publicação do Certificado 25
4.4.3. Notificação de Emissão de Certificado a Outras Entidades 25
4.5. Utilização do Certificado e Par de Chaves 25
4.5.1. Utilização do Certificado e da Chave Privada pelo Titular 25
4.5.2. Utilização do Certificado e da Chave Pública pelas Partes Confiantes 26
4.6. Renovação de Certificados 26
4.7. Renovação de Certificados com Geração de Novo Par de Chaves 27
4.7.1. Motivo para Renovação de Certificados com Geração de Novo Par de Chaves 27
4.7.2. Quem pode Pedir a Certificação de Nova Chave Pública 27
4.7.3. Processamento do Pedido de Certificação de Nova Chave Pública 27
4.7.4. Notificação de Emissão de Novo Certificado ao Titular 27
4.7.5. Procedimentos para Aceitação do Certificado Renovado com Novo Par de Chaves 27
4.7.6. Publicação do Certificado Renovado com Novo Par de Chaves 27
4.7.7. Notificação de Emissão de Certificado Renovado com Novo Par de Chaves a Outras Entidades 27
4.8. Modificação de Certificado 27
4.9. Suspensão e Revogação de Certificado 27
4.9.1. Motivos para a Revogação 28
4.9.2. Quem pode Pedir a Revogação 28
4.9.3. Procedimento para o Pedido de Revogação 28

4.9.4. Produção de Efeitos de um Pedido de Revogação 28
4.9.5. Prazo de Processamento de um Pedido de Revogação 28
4.9.6. Requisitos de Verificação de Revogação pelas Partes Confiantes 29
4.9.7. Frequência de Emissão das LCR 29
4.9.8. Período de Latência Máximo para as LCR 29
4.9.9. Disponibilidade de Revogações / Verificação do Estado On-Line 29
4.9.10. Requisitos de Verificação de Revogação On-Line 29
4.9.11. Outras Formas Disponíveis de Divulgação de Revogação 29
4.9.12. Requisitos Especiais Relativos ao Comprometimento de Chave 30
4.9.13. Motivos para Suspensão 30
4.9.14. Quem Pode Requerer a Suspensão 30
4.9.15. Procedimentos para Requerer a Suspensão 30
4.9.16. Limite do Período de Suspensão 30
4.10. Serviços de Estado do Certificado 30
4.10.1. Características Operacionais 30
4.10.2. Disponibilidade dos Serviços 30
4.10.3. Características Opcionais 30
4.11. Fim de Subscrição 30
4.12. Custódia e Recuperação de Chaves (Key-Escrow) 31
4.12.1. Políticas e Práticas de Custódia e Recuperação de Chaves 31
4.12.2. Políticas e Práticas de Encapsulamento e Recuperação de Chaves de Sessão 31
5. Instalações, Gestão e Controlos Operacionais 32
5.1. Controlos Físicos 32
5.1.1. Localização Física e Tipo de Construção 32
5.1.2. Acesso Físico 32
5.1.3. Eletricidade e Ar Condicionado 32
5.1.4. Exposição à Água 33
5.1.5. Prevenção e Proteção Contra Incêndios 33
5.1.6. Salvaguarda de suportes de Armazenamento 33
5.1.7. Eliminação de Resíduos 33
5.1.8. Instalações Externas para Recuperação de Segurança 33
5.2. Controlos Processuais 33
5.2.1. Funções de Confiança 33
5.2.2. Número de Pessoas Necessárias por Tarefa 34
5.2.3. Identificação e Autenticação para Cada Função 34
5.2.4. Funções que Necessitem de Segregação de Poderes 35
5.3. Controlos do Pessoal 35
5.3.1. Requisitos de Antecedentes, Qualificações, Experiência e Credenciação 35

5.3.2. Procedimentos de Verificação de Antecedentes 35
5.3.3. Requisitos de Instrução 36
5.3.4. Frequência e Requisitos de Instrução de Reciclagem 36
5.3.5. Frequência e Sequência de Rotação nas Funções 36
5.3.6. Sanções para Ações Não Autorizadas 37
5.3.7. Requisitos para Prestadores de Serviços 37
5.3.8. Documentação Fornecida ao Pessoal 37
5.4. Procedimentos de Registos de Auditoria 37
5.4.1. Tipo de Eventos Registados 37
5.4.2. Frequência da Auditoria de Registos 38
5.4.3. Período de Retenção dos Registos de Auditoria 38
5.4.4. Proteção dos Registos de Auditoria 38
5.4.5. Procedimentos para as Cópias de Segurança dos Registos de Auditoria 38
5.4.6. Sistema de Recolha de Registos 39
5.4.7. Notificação de Agentes Causadores de Eventos 39
5.4.8. Avaliação de Vulnerabilidades 39
5.5. Arquivo de Registos 39
5.5.1. Tipo de Registos Guardados 39
5.5.2. Período de Retenção em Arquivo 39
5.5.3. Proteção dos Arquivos 39
5.5.4. Procedimentos para as Cópias de Segurança dos Arquivos 39
5.5.5. Requisitos para Validação Cronológica dos Registos 39
5.5.6. Sistema de Recolha de Dados de Arquivo (Interno ou Externo) 40
5.5.7. Procedimentos para Obtenção e Verificação da Informação dos Arquivos 40
5.6. Renovação de Chaves 40
5.7. Comprometimento e Recuperação em caso de Desastre 40
5.7.1. Procedimentos em caso de Incidentes e Comprometimento 40
5.7.2. Corrupção de Recursos Informáticos, Software e/ou Dados 40
5.7.3. Procedimentos em caso de Comprometimento da Chave Privada da EC 40
5.7.4. Capacidade de Continuação da Atividade Após Desastre 40
5.8. Extinção da EC ou ER 41
6. Controlos de Segurança Técnica 42
6.1. Geração e Instalação do Par de Chaves 42
6.1.1. Geração do Par de Chaves 42
6.1.2. Entrega da Chave Privada ao Titular 42
6.1.3. Entrega da Chave Pública ao Emissor do Certificado 42
6.1.4. Entrega da Chave Pública da EC a Utilizadores e Partes Confiantes 42
6.1.5. Tamanho das Chaves 43
6.1.6. Geração de Parâmetros da Chave Pública 43

6.1.7. Utilização da Chave (KeyUsage) 43
6.2. Proteção da Chave Privada e Características dos Módulos Criptográficos 43
6.2.1. Normas para Módulos Criptográficos 43
6.2.2. Controlo Múlti-Pessoal (m de n) para a Chave Privada 43
6.2.3. Retenção da chave privada (key escrow) 43
6.2.4. Cópia de Segurança da Chave Privada 44
6.2.5. Arquivo da Chave Privada 44
6.2.6. Transferência da Chave Privada do/para o Módulo Criptográfico 44
6.2.7. Armazenamento da Chave Privada em Módulo Criptográfico 44
6.2.8. Método de Ativação da Chave Privada 44
6.2.9. Método de Desativação da Chave Privada 44
6.2.10. Método de Destruição da Chave Privada 44
6.2.11. Classificação do Módulo Criptográfico 44
6.3. Outros Aspetos da Gestão do Par de Chaves 45
6.3.1. Arquivo da Chave Pública 45
6.3.2. Períodos de Utilização de Chaves Públicas e Privadas 45
6.4. Dados de Ativação 45
6.4.1. Geração de Dados de Ativação e Instalação 45
6.4.2. Proteção de Dados de Ativação 46
6.4.3. Outros Aspetos de Dados de Ativação 46
6.5. Controlos de Segurança Informática 46
6.5.1. Requisitos Técnicos Específicos de Segurança Informática 46
6.5.2. Classificação da Segurança Informática 46
6.6. Controlos Técnicos do Ciclo de Vida 47
6.6.1. Controlos de Desenvolvimentos de Sistemas 47
6.6.2. Controlos de Gestão de Segurança 47
6.6.3. Classificação de Segurança do Ciclo de Vida 47
6.7. Controlos de Segurança da Rede 47
6.8. Validação cronológica (Time-stamping) 47
7. Perfis de Certificado e LCR 48
7.1. Perfil de Certificado 48
7.1.1. Número(s) de Versão 48
7.1.2. Extensões do Certificado 48
7.1.3. Identificadores de Algoritmo 50
7.1.4. Formato dos Nomes 51
7.1.5. Restrições aos Nomes 56
7.1.6. Identificador da Política de Certificados 56
7.1.7. Utilização da Extensão Policy Constraints 56
7.1.8. Sintaxe e Semântica dos Policy Qualifiers 56

7.1.9. Semântica de Processamento para a Extensão Crítica Certificate Policy 56
7.2. Perfil de LCR 57
7.2.1. Número(s) de Versão 57
7.2.2. Extensões da LCR 57
7.3. Perfil de OCSP 57
7.3.1. Número(s) de Versão 57
7.3.2. Extensões do OCSP 57
8. Auditorias e Avaliações de Conformidade 58
8.1. Frequência e Circunstâncias das Auditorias 58
8.2. Identidade/Qualificações do Auditor 58
8.3. Relação entre o Auditor e a Entidade Auditada 58
8.4. Âmbito da Auditoria 58
8.5. Ações Desenvolvidas como Resultado de Deficiências 58
8.6. Comunicação de Resultados 59
9. Outros Assuntos de Carácter Comercial e Legal 60
9.1. Honorários 60
9.1.1. Honorários por Emissão ou Renovação de Certificados 60
9.1.2. Honorários para Acesso aos Certificados 60
9.1.3. Honorários para Acesso à informação de Estado ou Revogação de Certificados 60
9.1.4. Honorários de Outros Serviços 60
9.1.5. Política de Reembolso 60
9.2. Responsabilidade Financeira 60
9.2.1. Cobertura do Seguro 60
9.2.2. Outros Recursos 60
9.3. Confidencialidade da Informação 61
9.3.1. Âmbito da Confidencialidade da Informação 61
9.3.2. Informação fora do Âmbito da Confidencialidade da Informação 61
9.3.3. Responsabilidades de Proteção da Confidencialidade da Informação 61
9.4. Privacidade da Informação Pessoal 61
9.4.1. Plano de Garantia de Privacidade 61
9.4.2. Informação Privada 61
9.4.3. Informação Considerada Não-Privada 61
9.4.4. Responsabilidades de Proteção da Informação Privada 62
9.4.5. Notificação e Consentimento de Utilização da Informação Privada 62
9.4.6. Divulgação por Imposição da Justiça 62
9.4.7. Outras Circunstâncias para Divulgação 62
9.5. Direitos de Propriedade Intelectual 62
9.6. Representações e Garantias 62

9.6.1. Representações e Garantias da EC 62
9.6.2. Representações e Garantias da ER 63
9.6.3. Representações e Garantias dos Titulares 63
9.6.4. Representações e Garantias das Partes Confiantes 63
9.7. Renúncia de Garantias 63
9.8. Limitações de Responsabilidade da EC 64
9.9. Indemnizações 64
9.10. Termo e Cessação 64
9.10.1. Termo 64
9.10.2. Cessação 64
9.11. Notificações Individuais e Comunicações 64
9.12. Alterações 65
9.12.1. Procedimento para Alterações 65
9.12.2. Mecanismos e Prazos de Notificação 65
9.12.3. Motivos para Alteração de Identificador 65
9.13. Disposições para Resolução de Conflitos 65
9.13.1. Resolução de Conflitos entre a DigitalSign e Clientes ER 65
9.13.2. Resolução de Conflitos com os Utilizadores ou Partes Confiantes 65
9.14. Lei Vigente 65
9.15. Conformidade com a Lei Vigente 66
9.16. Providências Várias 66
9.16.1. Acordo Completo 66
9.16.2. Independência 66
9.16.3. Severidade 66
9.16.4. Execuções 66
9.16.5. Força Maior 66
9.17. Outras Providências 66
9.17.1. Grupo de Gestão 66
10. Apêndice A – Acrónimos e Definições 67

1. INTRODUÇÃO

Em 31 de outubro de 2017, a DigiCert Inc. concluiu a aquisição da unidade de negócios de segurança de websites da Symantec. Como resultado, a DigiCert agora é a proprietária da Política de Certificados STN e dos Serviços PKI descritos neste documento.

No entanto, poderá haver referências a "VeriSign", "Symantec" e "DigiCert" neste documento até que seja operacionalmente prático concluir a renomeação das autoridades e serviços de certificação. Quaisquer referências à VeriSign ou à Symantec como uma entidade corporativa devem ser estritamente consideradas como linguagem herdada que reflete apenas o histórico de propriedade.

O objetivo deste documento é definir as práticas e procedimentos utilizados no suporte às atividades de certificação digital pela Entidade Certificadora da DigitalSign – Certificadora Digital, SA ("EC DIGITALSIGN").

Este documento – Declaração de Práticas de Certificação ("DPC") – é baseado na declaração de práticas de certificação da British Telecommunications plc e das práticas de certificação da Symantec/Digicert/Quovadis (disponíveis para consulta pública em: https://www.trustwise.com/repository/CPS/cps.htm), cumprindo toda a legislação Nacional e Comunitária aplicável, e a quem a DigitalSign subcontrata serviços de certificação eletrónica, de acordo com contratos estabelecidos entre as partes, conforme quadro seguinte:

Serviço	***Entidade Subcontratada***
Geração de certificados	British Telecomunications, plc
Estado das Revogações	British Telecomunications, plc
Data Center	British Telecomunications, plc

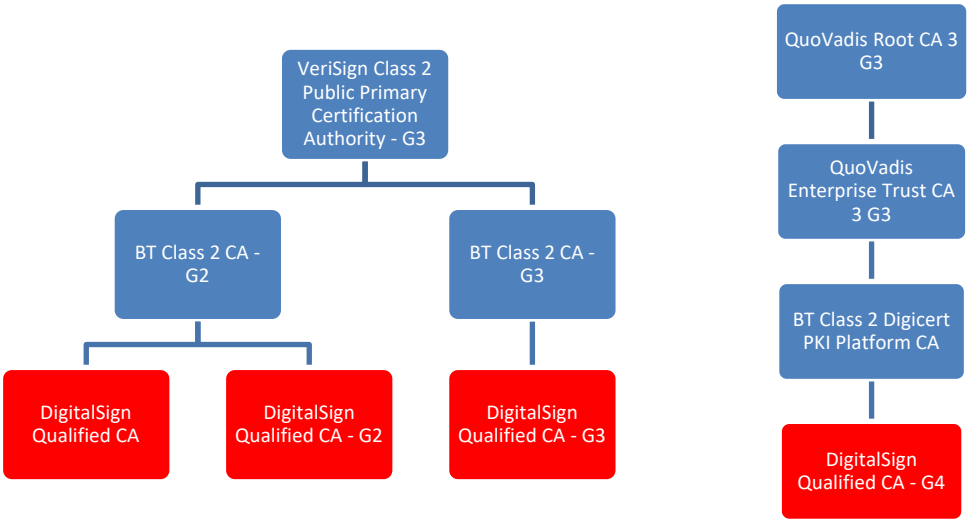
As entidades subcontratadas são responsáveis pela aplicação das normas e procedimentos constantes nesta DPC, no âmbito do fornecimento dos serviços subcontratados. O Grupo de Gestão, definido no ponto 9.17.1 deste documento, é responsável por garantir a efetiva implementação de todos os processos e procedimentos do sistema de gestão e analisar periodicamente a necessidade de readequação nos mesmos, numa lógica de melhoria contínua, através da análise crítica da sua eficácia.

Compete ainda a este grupo de gestão o acompanhamento regular da relação com as entidades subcontratadas, de acordo com o procedimento respetivo (PQ-06) de gestão de compras e que faz parte integrante do Sistema de Gestão da Qualidade.

Estabelece as práticas que a EC DIGITALSIGN emprega no fornecimento de serviços de certificação que incluem, mas que não estão limitadas à emissão, gestão, revogação e renovação de certificados qualificados, de acordo com os requisitos da Symantec Trust Network Certificate Policies ("CP").

A CP é a principal declaração de políticas de administração da STN. Estabelece os requisitos comerciais, legais e técnicos para aprovação, emissão, gestão, utilização, revogação e renovação de certificados digitais dentro da STN e providencia serviços associados de confiança. Estes requisitos, designados de 'Padrão STN', protegem a segurança e integridade da STN aplicáveis a todos os seus participantes e, como tal, fornecem garantias uniformes de total confiança. Mais informações relativas à STN e aos seus padrões estão disponíveis na CP.

A DigitalSign tem autoridade completa sobre uma parte desta STN, designada pelo seu subdomínio da STN. O subdomínio da DigitalSign inclui entidades a si subordinadas, tais como, Clientes, Utilizadores Finais e Partes Confiantes.



Os certificados emitidos por estas entidades certificadoras intermédias obtêm o reconhecimento obtido pela EC RAÍZ nas aplicações comerciais (leia-se: Browsers como o Internet Explorer, Google Chrome, Mozilla Firefox, etc.).

Enquanto a CP estabelece requisitos que os participantes da STN devem cumprir, esta DPC descreve como a DigitalSign cumpre estes requisitos dentro do subdomínio da STN de acordo com os requisitos da Legislação Portuguesa e Europeia aplicável. Especificamente esta DPC descreve as práticas que a DigitalSign emprega para:

- Gerir com segurança o núcleo das infraestruturas que suportam as operações
- Emitir, gerir, revogar e renovar Certificados Digitais Qualificados.

Para assuntos relacionados com o serviço de validação cronológica, em conjunto com esta DPC, deverá também ser consultado o documento "Políticas e Práticas de Certificação de Validação Cronológica", o qual se encontra disponível no repositório da EC DIGITALSIGN em: https://www.digitalsign.pt/ECDIGITALSIGN/cps.

Esta DPC está conforme a Internet Engineering Task Force (IETF) RFC 3647 para Políticas de Certificados e definição da Declaração de Prática de Certificação, podendo sofrer atualizações regulares.

1.1. CONTEXTUALIZAÇÃO

As práticas de criação, assinatura e emissão de certificados, assim como a revogação de certificados inválidos levadas a cabo por uma Entidade de Certificação ("EC") são fundamentais para garantir a fiabilidade e confiança de uma Infraestrutura de Chaves Públicas ("PKI").

Respeita e implementa os seguintes standards:

- RFC 3647: *Internet X.509 Public Key Infrastructure — Certificate Policy and Certification Practices Framework*

- RFC 3280: *Internet X.509 PKI - Certificate and CRL Profile*

Esta DPC satisfaz os requisitos impostos pela legislação Nacional e Comunitária aplicável a certificados qualificados e especifica como implementar os seus procedimentos e controlos, e ainda como a EC DIGITALSIGN atinge os requisitos especificados.

A DigitalSign, ao abrigo desta EC, apenas oferece certificados qualificados. A DPC descreve como a DigitalSign reúne os requisitos da CP para esta Classe de certificados, dentro do seu Subdomínio.

A DIGITALSIGN poderá publicar DPCs que sejam suplementares a esta, de modo a cumprir com requisitos políticos específicos do Governo, ou outros padrões e requisitos da indústria.

Esta política suplementar de certificados, deverá estar disponível aos subscritores dos certificados emitidos sob a mesma e às partes confiantes.

1.2. DESIGNAÇÃO E IDENTIFICAÇÃO DO DOCUMENTO

Este documento é a Declaração de Práticas de Certificação da EC DIGITALSIGN. Os certificados emitidos ao abrigo do padrão STN contêm um identificador de objeto correspondente à Classe de certificado da STN, pelo que a DigitalSign não associou nenhum identificador a esta DPC.

0 OID da Política de Certificado é utilizado de acordo com o explicitado na secção 7.1.6.

Este documento é identificado pela seguinte informação:

Informação do Documento	
Versão/Edição	3.7
Data de Aprovação	15/06/2021
Data de Validade	Não aplicável
Localização	https://www.digitalsign.pt/ECDIGITALSIGN/cps

1.3. PARTICIPANTES NA PKI

1.3.1. ENTIDADES CERTIFICADORAS

O termo "Entidade Certificadora" designa a entidade que emite e gere certificados digitais.

A EC DIGITALSIGN insere-se na hierarquia de confiança da Symantec/Digicert/Quovadis e da BT. A EC DIGITALSIGN emite certificados qualificados para pessoas singulares e coletivas e presta serviços necessários como a validação on-line OCSP.

A EC DIGITALSIGN é assinada pela BT, que por sua vez é assinada pela Symantec/Digicert/Quovadis.

1.3.2. ENTIDADES DE REGISTO

A Entidade de Registo (ER) é uma entidade que desempenha o papel de identificação e autenticação dos subscritores de certificados digitais, inicia ou encaminha pedidos de revogação e aprova aplicações para renovação de certificados em nome da EC. A DigitalSign pode agir como ER para os certificados que emite.

Terceiras partes, que entrem numa relação contratual com a DigitalSign, podem operar a sua própria ER e autorizar a emissão de certificados pela EC DIGITALSIGN. As ERs terceiras

devem respeitar, através de todos os requisitos, esta DPC e os termos do seu contrato com a DigitalSign. As ERs terceiras poderão implementar práticas mais restritivas, com base nos seus requisitos internos.

A identificação da ER, quando distinta da EC, deverá ser parte constante da informação no certificado digital qualificado, através de um identificador "OU" no campo "Assunto" (ex: OU = ER – Nome da Entidade).

1.3.3. TITULARES DOS CERTIFICADOS

Os titulares dos certificados são os utilizadores finais dos certificados emitidos por uma EC. Um titular é a entidade nomeada como o utilizador final subscritor de um certificado. Os subscritores podem ser indivíduos ou organizações, bem como para equipamentos tecnológicos como validação OCSP ou validação cronológica.

1.3.4. PARTES CONFIANTES

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

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

As partes confiantes podem ou não ser titulares de certificados emitidos na hierarquia de confiança da Symantec/Digicert/Quovadis (STN).

1.3.5. OUTROS PARTICIPANTES

Nenhum.

1.4. UTILIZAÇÃO DO CERTIFICADO

Os certificados emitidos pela EC DIGITALSIGN são utilizados, pelos diversos sistemas, aplicações, mecanismos e protocolos, com o objetivo de garantir os seguintes serviços de segurança:

- Controlo de acessos
- Integridade
- Autenticação
- Não-repúdio

Estes serviços são obtidos com recurso á utilização de criptografia de chave pública, através da sua utilização na infraestrutura de confiança que a EC DIGITALSIGN e STN / BT proporcionam. Os serviços de identificação e autenticação, integridade e não-repúdio são obtidos mediante a utilização de assinaturas ou selos eletrónicos.

1.4.1. UTILIZAÇÃO ADEQUADA DO CERTIFICADO

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

Os certificados atribuídos a pessoas singulares têm como objetivo a sua utilização em qualquer aplicação para efeitos de assinatura eletrónica qualificada.

Os certificados atribuídos a pessoas coletivas têm como objetivo a sua utilização em qualquer aplicação para efeitos de selo eletrónico qualificado.

Os certificados emitidos pela EC DIGITALSIGN são também utilizados pelas Partes Confiantes para verificação da sua cadeia de confiança, assim como para garantir a autenticidade e identidade do emissor de uma assinatura eletrónica ou selo eletrónico gerado pela chave privada correspondente á chave pública contida nesse certificado.

1.4.2. UTILIZAÇÃO NÃO AUTORIZADA

Os certificados devem apenas ser usados na medida em que seja consistente com a lei aplicável.

Os certificados emitidos pela EC DIGITALSIGN não são concebidos, destinados ou autorizados para o uso ou revenda em controlo de equipamentos em circunstâncias perigosas, ou para usos que necessitem de um desempenho à prova de falhas, como instalações nucleares, aviação, sistema de controlo de tráfego aéreo ou controlo de armas, em que uma falha possa levar diretamente à morte, lesão corporal ou graves prejuízos ambientais.

Os certificados EC não podem ser usados em nenhuma função, exceto as funções da EC. Adicionalmente, os certificados de utilizadores finais não podem ser usados como certificados EC.

1.5. GESTÃO DE POLÍTICAS

1.5.1. ENTIDADE RESPONSÁVEL PELA GESTÃO DO DOCUMENTO

DigitalSign – Certificadora Digital, SA.
Largo Padre Bernardino Ribeiro Fernandes, 26
4835-489 Nespereira – Guimarães
Portugal

1.5.2. CONTACTOS

Álvaro Matos
DigitalSign – Certificadora Digital, SA.
Largo Padre Bernardino Ribeiro Fernandes, 26
4835-489 Nespereira – Guimarães
Portugal
Email: suporte@digitalsign.pt
Telefone: +351 253560650
Fax: +351 253560639

1.5.3. DETERMINAÇÃO DE CONFORMIDADE

O grupo de trabalho desta política avalia a conformidade e aplicabilidade interna desta DPC (e/ou respetivas PCs), submetendo-a à aprovação da administração da DigitalSign, que é o órgão competente para determinar a sua adequação com a legislação aplicável.

1.5.4. PROCEDIMENTOS DE APROVAÇÃO

A aprovação interna desta DPC (e/ou respetivas PCs) e seguintes correções e/ou atualizações são efetuadas pelo grupo de trabalho desta política.

Após a aprovação interna, deverá ser determinada a sua conformidade, de acordo com o descrito no ponto anterior.

Fazendo parte de uma hierarquia de confiança, as correções e/ou atualizações a esta DPC deverão ser também validadas pela AC emissora do certificado da EC DIGITALSIGN (a British Telecomunications Plc).

As correções e/ou atualizações deverão ser publicadas sob a forma de novas versões desta DPC (e/ou respetivas PCs), substituindo qualquer versão anterior.

1.6. ACRÓNIMOS E DEFINIÇÕES

Ver Apêndice A.

2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIOS

2.1. REPOSITÓRIOS

A DigitalSign é responsável pelas funções de repositório da sua própria EC DIGITALSIGN. A DigitalSign publica todos os certificados que emite no repositório, de acordo com a secção 2.2.

Após revogação de um certificado, a DigitalSign publica notificação de tal revogação no repositório. A DigitalSign emite Listas de Certificados Revogados (LCRs) para o seu subdomínio da STN, ao abrigo do disposto nesta DPC. Adicionalmente, para clientes que tenham contratado o Online Status Certificate Protocol (OSCP), a DigitalSign fornece o serviço OSCP, ao abrigo do disposto nesta DPC.

2.2. PUBLICAÇÃO DA INFORMAÇÃO DOS CERTIFICADOS

A DigitalSign mantém um repositório Web-based, que permite às partes confiantes efetuar inquéritos e pesquisas online relativas às revogações e outras informações sobre o estado dos certificados. A DigitalSign fornece informações às partes confiantes, sobre como encontrar o repositório apropriado para verificar o estado dos certificados e, se o Online Certificate Status Protocol (OSCP) estiver disponível, como encontrar o OSCP correspondente.

A DigitalSign publica no seu repositório os certificados que emite e, aquando da revogação de um certificado, publica a notificação de tal revogação. Adicionalmente, a DigitalSign emite Listas de Certificados Revogados e, se disponível, fornece serviços de OCSP para a EC DIGITALSIGN.

A DigitalSign é responsável pelas funções de repositório para a EC DIGITALSIGN.

A DigitalSign publica sempre, e pelo menos, a seguinte informação pública on-line:

- Cópia eletrónica desta DPC (https://www.digitalsign.pt/ECDIGITALSIGN/cps)
- LCRs:
  - Para certificados emitidos pela EC "DigitalSign Qualified CA": (http://onsitecrl.trustwise.com/DigitalSignCertificadoraDigitalQualifiedCertificate/LatestCRL.crl)
  - Para certificados emitidos pela EC "DigitalSign Qualified CA – G2": (http://onsitecrl.trustwise.com/DigitalSignCertificadoraDigitalQualifiedCertificateG2/LatestCRL.crl)
  - Para certificados emitidos pela EC "DigitalSign Qualified CA – G3": (http://onsitecrl.trustwise.com/DigitalSignCertificadoraDigitalQualifiedCertificateG3/LatestCRL.crl)
  - Para certificados emitidos pela EC "DigitalSign Qualified CA – G4": (http://onsitecrl.trustwise.com/DigitalSignCertificadoraDigitalQualifiedCertificateG4/LatestCRL.crl)

2.3. PERIODICIDADE DE PUBLICAÇÃO

As atualizações desta DPC e PC são publicadas de acordo com a secção 9.12.

Os certificados são publicados após emissão. A LCR é publicada diariamente.

Informação adicional sobre o estado do certificado é publicada de acordo com as disposições desta DPC.

2.4. CONTROLO DE ACESSOS AOS REPOSITÓRIOS

A informação publicada no repositório da DigitalSign está publicamente disponível, sendo garantido e sem restrições o acesso de leitura.

A DigitalSign implementou medidas de segurança lógica e física, para prevenir que pessoas não autorizadas adicionem, apaguem ou modifiquem as entradas dos repositórios.

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1. ATRIBUIÇÃO DE NOMES

A atribuição de nomes segue o disposto na legislação aplicável, sendo que para os certificados emitidos a pessoas singulares e coletivas é atribuído o seu nome real.

3.1.1. TIPOS DE NOMES

Os certificados emitidos pela EC DIGITALSIGN são identificados por um nome único nos campos Emissor e Assunto, denominado *Distinguished Name – DN*, de acordo com a norma X.501.

Os DN consistem no especificado na tabela seguinte:

Atributo	***Valor***
País (Country – "C")	"PT", ou outro de acordo com a tabela ISO 3166
Organização (Organization – "O")	Nome da empresa ou instituição à qual pertence o titular da assinatura (onde aplicável)
Unidade Organizacional (Organizational Unit – "OU")	Os certificados digitais podem conter vários atributos OU, de acordo com o PC correspondente
Distrito (State or Province – "S")	O Distrito do titular da assinatura, ou não usado
Localidade (Locality – "L")	A Localidade do titular da assinatura, ou não usado
Nome Comum (Common Name – "CN")	Titular do certificado, serviço ou empresa que o titular representa
Endereço de E-Mail (Email Address – "E")	Endereço de email associado ao titular da assinatura (onde aplicável)
Primeiro Nome (Given Name – "G")	Primeiro(s) nome(s) do titular do certificado, quando emitido para pessoas singulares ou não usado
Apelido (Surname – "SN")	Apelido(s) do titular do certificado, quando emitido para pessoas singulares ou não usado
ID (SERIALNUMBER)	Identificador do titular do certificado, quando emitido para pessoas singulares ou não usado
ID (Organization Identifier)	Identificador da organização, ou não usado
Título (Title – "T")	Título profissional ou outro utilizado pelo titular do certificado

3.1.2. NECESSIDADE DE NOMES SIGNIFICATIVOS

A EC DigitalSign irá assegurar, dentro do seu subdomínio na hierarquia de confiança da STN:

- A singularidade da informação constante do DN
- Todos os dados incluídos no campo DN são devidamente validados e autenticados, sendo facilmente percetíveis e identificáveis pelos Humanos, permitindo a determinação inequívoca do respetivo titular.

3.1.3. ANONIMATO OU PSEUDÓNIMOS DOS TITULARES

Os titulares dos certificados qualificados podem usar pseudónimos (outros nomes que não o seu verdadeiro nome). Neste caso, a indicação de que está a ser usado um pseudónimo será indicada no campo "Observações".

Não é autorizado o anonimato.

Apenas quando as restrições técnicas inerentes aos tamanhos máximos definidos para cada campo sejam limitativas de conter a totalidade da informação, poderão ser autorizadas abreviaturas, desde que as mesmas sejam facilmente percetíveis e identificáveis pelos Humanos.

3.1.4. REGRAS PARA INTERPRETAÇÃO DOS VÁRIOS FORMATOS DE NOMES

Não estipulados.

3.1.5. SINGULARIDADE DOS NOMES

A DigitalSign assegura que os dados constantes do DN são únicos dentro da sua EC, através de componentes automatizadas no processo de inscrição dos titulares. É possível a um titular ter dois ou mais certificados com o mesmo DN.

3.1.6. RECONHECIMENTO, AUTENTICAÇÃO E FUNÇÃO DAS MARCAS REGISTADAS

As entidades requisitantes de certificados têm demonstrar o direito á utilização do nome requisitado, não podendo as designações usadas nos certificados emitidos pela EC DIGITALSIGN infringir os direitos de propriedade intelectual de outros.

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

A DigitalSign não arbitra, media, ou de qualquer outra forma resolve qualquer disputa relacionada com a titularidade de qualquer nome ou marca. A DigitalSign reserva o direito, sem responsabilidade para com qualquer subscritor de certificado, a rejeitar qualquer pedido devido a tais disputas.

3.2. VALIDAÇÃO INICIAL DE IDENTIDADE

Para todos os certificados, é obrigatório que o registo inicial seja efetuado presencialmente ou de forma equivalente, de forma a garantir que a pessoa a quem vai ser emitido o certificado é de facto quem diz ser.

O processo de validação de identidade pode ser conseguido através de três formas alternativas:

a) presencialmente na DigitalSign (ou ER autorizada); ou

b) apresentação de documentos que para a sua obtenção foi exigida a presença física, como é o caso do BI ou CC, complementado com o respetivo reconhecimento da assinatura por Notário (ou entidade equivalente, nos termos legais em vigor); ou

c) através de videoconferência remota.

Estas práticas estão de acordo com o documento ETSI EN 319 411-2 e de acordo com a legislação em vigor.

Nesta DPC são descritos todos os passos necessários, desde o início do pedido de certificado até á atribuição do certificado digital ao seu titular.

3.2.1. MÉTODO PARA PROVA DE POSSE DA CHAVE PRIVADA

A DigitalSign usa vários circuitos para emitir certificados nos quais a chave privada é gerida de forma diferente. A chave privada pode ser criada pelo titular ou pela DigitalSign.

O método usado para a criação de chave é visível no certificado, através da identificação da política e do atributo no campo DN do certificado. Esses códigos são descritos nas políticas correspondentes e nos registros de perfil de certificado.

a) Chaves criadas pela DigitalSign:
   As chaves podem ser entregues pela DigitalSign ao Titular/Signatário, diretamente ou através de uma autoridade de registro, num dispositivo de criação de assinatura qualificado (QSCD).

b) Chaves criadas pelo signatário:
   A prova de propriedade da chave privada neste caso é a solicitação que a DigitalSign recebe no formato PKCS#10

3.2.2. AUTENTICAÇÃO DE IDENTIDADE DE UMA PESSOA COLETIVA

O processo de autenticação de identidade de uma pessoa coletiva deve obrigatoriamente garantir que a pessoa coletiva para quem vai ser emitido o certificado existe, sendo essa verificação efetuada por consulta a documentação oficial, exigindo-se a intervenção das pessoas singulares que, estatutariamente, representam essa pessoa coletiva.

Qualquer informação adicional incluída no DN é igualmente verificada e autenticada pelos serviços de validação.

3.2.3. AUTENTICAÇÃO DE IDENTIDADE DE UMA PESSOA SINGULAR

O processo de autenticação da identidade de uma pessoa singular garante que a pessoa singular para quem vai ser emitido o certificado é quem na realidade diz ser, através da submissão de documentação comprovativa e respetiva assinatura. Isso pode ser feito de três formas distintas:

a) presencialmente na DigitalSign (ou ER autorizada); ou
b) apresentação de documentos que para a sua obtenção foi exigida a presença física, como é o caso do BI ou CC, complementado com o respetivo reconhecimento da assinatura por Notário (ou entidade equivalente, nos termos legais em vigor); ou
c) através de videoconferência remota.

A verificação da identidade e poderes do representante/procurador (se aplicável) poderá ser efetuada indiretamente por via documental, por notário ou entidade com poderes legais para o reconhecimento de assinaturas na qualidade e com poderes para o ato.

Qualquer informação adicional incluída no DN é igualmente verificada e autenticada pelos serviços de validação.

3.2.4. INFORMAÇÃO DO TITULAR NÃO VERIFICADA

Toda a informação incluída no DN é verificada e autenticada pelos serviços de validação.

3.2.5. VALIDAÇÃO DE AUTORIDADE

São verificadas todas as informações relativas a poderes de representação e/ou afiliação de uma pessoa singular à correspondente empresa ou organização.

3.2.6. CRITÉRIOS PARA INTEROPERABILIDADE

A DigitalSign não disponibiliza serviços de interoperabilidade que permitam ECs não-STN interoperar com ECs STN através da certificação dessas ECs.

A interoperabilidade entre ECs STN está garantida pela própria hierarquia de confiança, sendo a raiz (Symantec/Digicert/Quovadis) automaticamente disponibilizada pela esmagadora maioria dos browsers, equipamentos e outros softwares existentes a nível global.

3.3. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDO DE RENOVAÇÃO DE CHAVES

Previamente à expiração de um certificado existente, é necessário renovar esse certificado, para que o titular (ou seu representante) mantenha a continuidade da sua utilização.

A DigitalSign requer que para o efeito seja criado um novo par de chaves, para substituir o par de chaves expirante (tecnicamente definido como «re-key», mas neste documento identificado como «renovação»).

O processo de criação do novo par de chaves pode ser conduzido internamente pela DigitalSign, ou diretamente pelo titular do certificado, sendo garantida a criação das mesmas no dispositivo criptográfico homologado. Neste caso é também requerido o conhecimento da "frase de identificação" definida pelo titular aquando do pedido inicial.

A verificação da identidade e demais dados constantes no DN é verificada sempre pelos serviços de validação da DigitalSign, de acordo com o disposto a seguir:

- Caso a informação constante do processo de renovação seja idêntica à informação constante do processo de autenticação inicial, e que essa autenticação tenha sido efetuada à menos de 2 (dois) anos, o pedido é automaticamente aprovado, sem necessidade de submissão de documentação ou prova de identidade adicional.
- Caso a informação constante do processo de renovação não seja idêntica à informação constante do processo de autenticação inicial, ou essa autenticação tenha sido efetuada à mais de 2 (dois) anos, o processo é tratado como um pedido inicial, sendo-lhe aplicáveis todas as regras de autenticação e validação descritas na secção 3.2.

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

Não existe renovação de chaves, de rotina.

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

Não é permitida a renovação de um certificado após este ter sido revogado, sendo sempre aplicáveis as regras de autenticação e validação descritas na secção 3.2.

No entanto, os documentos e informações constantes do pedido inicial podem ser utilizados para o efeito, desde que permaneçam válidos.

3.4. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDO DE REVOGAÇÃO

Previamente à revogação de um Certificado, a DigitalSign verifica se a revogação foi requerida pelo titular do certificado ou pela entidade que aprovou o pedido.

Os procedimentos aceites para autenticar os pedidos de revogação incluem:

- Solicitar ao titular a "frase de identificação", e revogar o certificado de forma automática, se coincidir com os registos existentes
- Receber uma mensagem, supostamente do seu titular, que peça a revogação e que contenha a assinatura digital verificável, com referência ao certificado a ser revogado
- Solicitação escrita do seu titular

Adicionalmente, a DigitalSign poderá proceder à revogação de um qualquer certificado, desde que tenha conhecimento (e após verificação) de que a informação constante do DN já não corresponde à realidade atual.

4. REQUISITOS OPERACIONAIS

4.1. PEDIDO DE CERTIFICADO

4.1.1. QUEM PODE SUBSCREVER UM PEDIDO DE CERTIFICADO

Os Pedidos subscrição de Certificados podem ser submetidos por:

- Um indivíduo que seja o titular do certificado
- Um representante do titular do certificado, devidamente autorizado e com poderes para o efeito
- Uma pessoa coletiva que seja o titular do certificado
- Um representante da EC DIGITALSIGN
- Um representante autorizado de uma ER

4.1.2. PROCESSO DE INSCRIÇÃO E RESPONSABILIDADES

4.1.2.1. CERTIFICADOS PARA UTILIZADORES FINAIS

Todos os utilizadores finais de certificados devem concordar com o disposto no "Acordo de Subscritor", que contém representações e garantias descritas na secção 9.6.3. e submeter-se a um processo de inscrição que consiste em completar um Formulário de Candidatura e fornecer informação verdadeira e correta, e todos os documentos de suporte necessários à validação das informações constantes no certificado.

Para processos de renovação, pode:

- Criar um par de chaves em dispositivo criptográfico homologado (conforme disposto na secção 3.3)
- Submeter a sua chave pública através das ferramentas disponibilizadas pela ER
- Demonstrar posse e/ou controle exclusivo da chave privada correspondente à chave pública entregue

4.1.2.2. CERTIFICADOS PARA ER

As entidades que desejem constituir-se como ER estão sujeitas à celebração de um contrato com a DigitalSign.

As ER devem fornecer as suas credencias para demonstrar a sua identidade e fornecer contacto para informações durante o processo de contratação. Durante este processo, o candidato a ER deve cooperar com a DigitalSign, para determinar o conteúdo dos certificados a serem emitidos pelo candidato.

4.2. PROCESSAMENTO DO PEDIDO DE CERTIFICADO

4.2.1. FUNÇÕES DE IDENTIFICAÇÃO E AUTENTICAÇÃO

A DigitalSign, ou uma ER, devem executar a identificação e autenticação de todos os pedidos, de Acordo com a secção 3.2.

4.2.2. APROVAÇÃO OU RECUSA DE PEDIDOS DE CERTIFICADO

A DigitalSign, ou uma ER, aprovarão os pedidos de certificado se os seguintes critérios forem cumpridos:

- Identificação e autenticação bem sucedida de toda a informação, nos termos da secção 3.2
- Logo que o pagamento seja efetuado ou aprovado

Caso se trate de um processo inicial, a ER efetuará a inicialização e personalização (se aplicável) do dispositivo criptográfico, onde efetuará a geração do par de chaves, e subsequente pedido de emissão à EC DIGITALSIGN.

Analogamente, nos casos de renovação onde o titular delegue a criação do par de chaves à ER, deverá esta efetuar essa geração no dispositivo criptográfico, e subsequente pedido de emissão à EC DIGITALSIGN.

Nos casos de renovação onde a geração do par de chaves seja efetuada pelo titular do certificado, a ER efetuará a aprovação do pedido.

A DigitalSign, ou uma ER, rejeitam o pedido de um certificado se qualquer uma das seguintes situações ocorrer:

- A identificação e autenticação, nos termos da secção 3.2, não estiver completa
- O subscritor não entregar toda a documentação de suporte pedida
- O subscritor não responder a notificações dentro de um prazo especificado
- Pagamento não seja executado
- A ER crer que emitir um certificado ao subscritor possa trazer descrédito à STN e à própria DigitalSign.

4.2.3. PRAZO PARA PROCESSAMENTO DO PEDIDO DE CERTIFICADO

A DigitalSign inicia o processamento dos pedidos após receção da documentação necessária. Não existe tempo estipulado para completar o processo, a não ser que de outra forma seja indicada relevância no acordo de subscritor, DPC ou outro acordo entre os participantes. Um pedido mantém-se ativo até ser rejeitado.

4.3. EMISSÃO DE CERTIFICADO

4.3.1. PROCEDIMENTOS PARA EMISSÃO DE CERTIFICADO

Um certificado é criado e emitido na sequência da aprovação de um pedido de certificado por qualquer uma das ER. A DigitalSign cria e emite ao titular (ou seu representante) um certificado baseado na informação recebida, suportado em documentos legais e na sequência da aprovação do mesmo por parte da ER.

Cada certificado emitido inicia a sua vigência (validade) no momento da sua emissão.

4.3.2. NOTIFICAÇÃO DE EMISSÃO DE CERTIFICADO AO TITULAR

A notificação de emissão do certificado ao seu titular (ou seu representante) é efetuada através de carta de acompanhamento aquando do envio do mesmo (e correspondente dispositivo criptográfico).

Nos casos de renovação (com criação do par de chaves pelo próprio) o titular é notificado através de mensagem de correio eletrónico, a qual inclui também instruções de instalação.

4.4. ACEITAÇÃO DO CERTIFICADO

4.4.1. PROCEDIMENTOS PARA ACEITAÇÃO DO CERTIFICADO

Conjuntamente com a notificação de emissão, conforme secção 4.3.2, é também remetido ao titular o "Termo de Receção", que terá obrigatoriamente de ser assinado pelo próprio ou seu(s) representante(s) legal(ais).

Apenas quando verificada a conformidade da assinatura, será remetido o código de acesso ao dispositivo criptográfico, necessário para a utilização da correspondente chave privada.

Esta situação não se aplica nos casos de renovação com criação do par de chaves pelo próprio, quando o certificado for destinado a equipamentos, ou quando for usada a solução de assinatura remota onde o processo de aceitação fica concluído no caso do titular não se opor ao certificado ou ao seu conteúdo.

4.4.2. PUBLICAÇÃO DO CERTIFICADO

A DigitalSign publica os certificados emitidos num repositório publicamente acessível.

4.4.3. NOTIFICAÇÃO DE EMISSÃO DE CERTIFICADO A OUTRAS ENTIDADES

As ER podem receber notificação da emissão dos certificados por si aprovados.

4.5. UTILIZAÇÃO DO CERTIFICADO E PAR DE CHAVES

4.5.1. UTILIZAÇÃO DO CERTIFICADO E DA CHAVE PRIVADA PELO TITULAR

O uso da chave privada correspondente à chave pública no certificado, deve apenas ser permitido quando o titular acordar e aceitar o contrato de subscrição do certificado. Este deve ser usado licitamente, de acordo com o contrato de subscrição da DigitalSign, nos termos deste DPC.

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.

Os certificados de validação cronológica têm como objetivo a sua utilização em servidores de validação cronológica.

Os titulares devem proteger a sua chave privada contra o uso não autorizado, e devem suspender o uso da chave privada na sequência da expiração ou revogação do certificado.

4.5.2. UTILIZAÇÃO DO CERTIFICADO E DA CHAVE PÚBLICA PELAS PARTES CONFIANTES

As Partes Confiantes devem estar em concordância com os termos estabelecidos nesta DPC e na respetiva política de certificação, como condição de confiança no certificado.

Antes de qualquer ato de confiança, as partes confiantes devem independentemente avaliar:

- A adequação do uso do certificado para quaisquer propósitos, e determinar que o certificado será, de facto, usado para propósitos adequados que não sejam proibidos, ou de outra forma restritos por esta DPC. A DigitalSign não é responsável por avaliar a devida adequação do uso do certificado.
- Se o certificado está a ser usado de acordo com o especificado no campo "*KeyUsage*" incluído no certificado (ex.: se a assinatura digital não é ativada, então o certificado pode não ser confiável para validação da assinatura do titular).
- O estado do certificado e de todas as EC na cadeia de certificação que emitiu o certificado. Se qualquer um dos certificados da cadeia de certificação está revogado, a parte confiante é unicamente responsável por avaliar se é razoável a confiança numa assinatura digital, efetuada em data anterior à revogação. Tal confiança é totalmente da responsabilidade da parte confiante.
- Ter conhecimento e perceber a utilização e funcionalidades proporcionadas pela criptografia de chave pública e certificados.
- Ler e perceber os termos e as condições descritas nas políticas e práticas de certificação.

Supondo que o uso do certificado é adequado, as partes confiantes devem utilizar o software e/ou o hardware apropriado para desempenhar a verificação da assinatura eletrónica ou selo eletrónico, ou outras operações criptográficas que desejem efetuar, com a condição de confiar nos certificados em conexão com tais operações. Tais operações incluem identificar a cadeia de certificados e verificar a assinatura digital em todos os certificados da mesma.

4.6. RENOVAÇÃO DE CERTIFICADOS

A renovação de um certificado com recurso ao mesmo par de chaves não é aceitável pela EC DIGITALSIGN.

4.7. RENOVAÇÃO DE CERTIFICADOS COM GERAÇÃO DE NOVO PAR DE CHAVES

A DigitalSign requer que para o efeito seja criado um novo par de chaves, para substituir o par de chaves expirante (tecnicamente definido como «re-key», mas neste documento identificado como «renovação»).

4.7.1. MOTIVO PARA RENOVAÇÃO DE CERTIFICADOS COM GERAÇÃO DE NOVO PAR DE CHAVES

Previamente à expiração de um certificado existente, é necessário renovar esse certificado, para que o titular (ou seu representante) mantenha a continuidade da sua utilização.

Um certificado pode ser renovado após a sua expiração.

4.7.2. QUEM PODE PEDIR A CERTIFICAÇÃO DE NOVA CHAVE PÚBLICA

Ver secção 4.1.1.

4.7.3. PROCESSAMENTO DO PEDIDO DE CERTIFICAÇÃO DE NOVA CHAVE PÚBLICA

Ver secção 4.1.2 e 4.2.

4.7.4. NOTIFICAÇÃO DE EMISSÃO DE NOVO CERTIFICADO AO TITULAR

Ver secção 4.3.2.

4.7.5. PROCEDIMENTOS PARA ACEITAÇÃO DO CERTIFICADO RENOVADO COM NOVO PAR DE CHAVES

Ver secção 4.4.1.

4.7.6. PUBLICAÇÃO DO CERTIFICADO RENOVADO COM NOVO PAR DE CHAVES

Ver secção 4.4.2.

4.7.7. NOTIFICAÇÃO DE EMISSÃO DE CERTIFICADO RENOVADO COM NOVO PAR DE CHAVES A OUTRAS ENTIDADES

Ver secção 4.4.3.

4.8. MODIFICAÇÃO DE CERTIFICADO

Esta é uma prática não suportada pela EC DIGITALSIGN.

4.9. SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO

A revogação ou suspensão de certificado é apenas aplicável se efetuada dentro do período de validade do certificado, e na prática significa que o mesmo perde a sua operacionalidade.

Os certificados revogados não podem ser reativados, i.e., voltar a ser válidos.

A EC DIGITALSIGN não suporta a suspensão de certificado.

4.9.1. MOTIVOS PARA A REVOGAÇÃO

Apenas nas circunstâncias abaixo indicadas, um certificado é revogado e publicado na LCR:

- Comprometimento ou suspeitas de que tenha havido comprometimento da chave privada.
- A DigitalSign ou ER tiverem razões para acreditar que um titular tenha violado uma obrigação ou garantia, ao abrigo do contrato aplicado.
- O contrato com o titular tenha terminado.
- A informação constante do DN já não corresponde à realidade atual.
- Existam razões para acreditar que o certificado foi emitido de uma forma desconforme com os procedimentos requeridos e aplicáveis pela DPC.
- Os dados constantes do DN são falsos.
- Por resolução judicial ou administrativa.
- Perda, destruição ou deterioração do dispositivo de suporte da chave privada.
- Revogação da EC DIGITALSIGN ou qualquer outra EC na cadeia de certificação.
- A continuação do uso desse certificado possa ser prejudicial para a DigitalSign e para a STN.

Para que o uso do certificado seja considerado prejudicial quando, são consideradas, de entre outras:

- A natureza e número de queixas recebidas.
- A identidade do(s) queixoso(s).
- A legislação relevante em vigor.
- As respostas ao alegado uso prejudicial do titular.

Os contratos de subscrição de certificados com a DigitalSign requerem que os titulares (ou seus representantes notifiquem imediatamente a DigitalSign (ou correspondente ER) se tiverem conhecimento, ou suspeitas, de que a sua chave privada esteja comprometida.

4.9.2. QUEM PODE PEDIR A REVOGAÇÃO

Os titulares podem pedir a revogação dos seus próprios certificados. A entidade que aprovou o certificado (ER) também pode pedir a revogação do certificado que aprovou.

4.9.3. PROCEDIMENTO PARA O PEDIDO DE REVOGAÇÃO

Ver secção 3.4.

4.9.4. PRODUÇÃO DE EFEITOS DE UM PEDIDO DE REVOGAÇÃO

Os pedidos de revogação devem ser submetidos o mais rapidamente possível. Após terem sido efetuados todos os procedimentos e seja verificado que o pedido é válido, o pedido não pode ser anulado.

4.9.5. PRAZO DE PROCESSAMENTO DE UM PEDIDO DE REVOGAÇÃO

A DigitalSign (ou ER) deve tratar estes pedidos de forma prioritária. A atualização do estado de revogação será efetuada num período de tempo máximo de 8 Horas úteis.

4.9.6. REQUISITOS DE VERIFICAÇÃO DE REVOGAÇÃO PELAS PARTES CONFIANTES

As partes confiantes devem verificar o estado dos certificados de que desejam confiar. Um dos métodos usados pelas partes confiantes é consultar a LCR mais recente, publicada pela EC que emite o certificado correspondente.

Em alternativa as partes confiantes podem cumprir este requisito, quer verificando o estado do certificado utilizando o repositório, na internet, ou o OSCP (quando disponível) para verificar o estado de revogação.

4.9.7. FREQUÊNCIA DE EMISSÃO DAS LCR

A LCR é emitida pelo menos uma vez por dia, para certificados de utilizador final. A LCR para Certificados EC deve ser emitida pelo menos anualmente, mas também sempre que uma EC é revogada.

Se um certificado listado na LCR expirar, pode ser removido das LCR emitidas posteriormente à expiração do certificado.

4.9.8. PERÍODO DE LATÊNCIA MÁXIMO PARA AS LCR

Após a criação de LCR, estas são publicadas no repositório dentro de um período muito breve. Normalmente tal é realizado automaticamente dentro de minutos após a criação.

4.9.9. DISPONIBILIDADE DE REVOGAÇÕES / VERIFICAÇÃO DO ESTADO ON-LINE

As revogações e outras informações sobre o estado dos certificados estão disponíveis através do repositório web-based e, quando existente, através do serviço OCSP. Adicionalmente à publicação de LCR, a DigitalSign fornece informação sobre o estado do certificado através de funções de inquérito no repositório da DigitalSign.

A informação do estado do certificado está disponível através de funções de inquérito na internet, acessíveis através do repositório da DigitalSign em:

- Para certificados emitidos pela EC "DigitalSign Qualified CA": (https://onsite.trustwise.com/services/DigitalSignCertificadoraDigitalQualifiedCertificate/client/search.htm)
- Para certificados emitidos pela EC "DigitalSign Qualified CA – G2": (https://onsite.trustwise.com/services/DigitalSignCertificadoraDigitalQualifiedCertificateG2/client/search.htm)
- Para certificados emitidos pela EC "DigitalSign Qualified CA – G3": (https://onsite.trustwise.com/services/DigitalSignCertificadoraDigitalQualifiedCertificateG3/client/search.htm)
- Para certificados emitidos pela EC "DigitalSign Qualified CA – G4": (https://onsite.trustwise.com/services/DigitalSignCertificadoraDigitalQualifiedCertificateG4/client/search.htm)

A DigitalSign também fornece serviços OCSP. Os clientes que contrataram esses serviços devem verificar o estado do certificado através do uso do OCSP. A URL para OCSP é comunicado ao cliente.

4.9.10. REQUISITOS DE VERIFICAÇÃO DE REVOGAÇÃO ON-LINE

As partes confiantes devem dispor de software/hardware capaz de aceder às informações disponibilizadas sobre o estado de revogação dos certificados.

4.9.11. OUTRAS FORMAS DISPONÍVEIS DE DIVULGAÇÃO DE REVOGAÇÃO

Não aplicável.

4.9.12. REQUISITOS ESPECIAIS RELATIVOS AO COMPROMETIMENTO DE CHAVE
A DigitalSign utilizará todos os esforços comercialmente razoáveis para notificar potenciais partes confiantes, se descobrir, ou tiver razões para acreditar que a chave privada da sua EC esteja comprometida.

4.9.13. MOTIVOS PARA SUSPENSÃO
Não aplicável.

4.9.14. QUEM PODE REQUERER A SUSPENSÃO
Não aplicável.

4.9.15. PROCEDIMENTOS PARA REQUERER A SUSPENSÃO
Não aplicável.

4.9.16. LIMITE DO PERÍODO DE SUSPENSÃO
Não aplicável.

4.10. SERVIÇOS DE ESTADO DO CERTIFICADO

4.10.1. CARACTERÍSTICAS OPERACIONAIS
O estado dos certificados públicos está disponível publicamente através das LCR e via OSCP responder (onde disponível).

4.10.2. DISPONIBILIDADE DOS SERVIÇOS
Os serviços de estado do certificado estão disponíveis 24 x 7, sem nenhuma interrupção programada.

4.10.3. CARACTERÍSTICAS OPCIONAIS
O OSCP é um serviço de recurso opcional que necessita de ser especificamente ativado.

4.11. FIM DE SUBSCRIÇÃO
Um titular pode terminar a subscrição de um certificado da seguinte forma:

- Deixando que o seu certificado expire, sem o renovar.
- Revogando o certificado antes do certificado expirar, sem o substituir.

4.12. CUSTÓDIA E RECUPERAÇÃO DE CHAVES (KEY-ESCROW)

A custódia de chaves privadas de ACs, ARs e de utilizadores finais não é permitida ao abrigo desta DPC.

A DigitalSign não armazena ou arquiva a chave privada de um Signatário destinada a criar assinatura/selo eletrônico, exceto no caso de certificação remota de um certificado qualificado através da solução de assinatura remota da DigitalSign.

Nesse caso, a chave privada é gerada num dispositivo qualificado de criação de assinatura (QSCD) e cifrada em um ambiente confiável. A cifra da chave é baseada numa chave simétrica AES (128 bits) criada pelo QSCD e derivada da *master wrapping key* do QSCD e do primeiro fator de autenticação criado/definido pelo Signatário, o que garante que somente ele/ela possa aceder a esse chave em particular.

4.12.1. POLÍTICAS E PRÁTICAS DE CUSTÓDIA E RECUPERAÇÃO DE CHAVES

A chave privada da EC DIGITALSIGN foi gerada e está armazenada em hardware de segurança (HSM) devidamente homologado, sendo garantida a sua salvaguarda (cópia de segurança) em dispositivo idêntico.

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

Não aplicável.

5. INSTALAÇÕES, GESTÃO E CONTROLOS OPERACIONAIS

5.1. CONTROLOS FÍSICOS

A DigitalSign implementou uma Política de Segurança, a qual apoia os requisitos de segurança deste DPC. A adequação com estas políticas está incluída nos requisitos de auditoria independente da DigitalSign descritos na secção 8. A Política de Segurança da DigitalSign contém informação sensível de segurança, estando apenas disponível através de acordos com a DigitalSign. Uma visão geral dos requisitos estão descritos abaixo.

5.1.1. LOCALIZAÇÃO FÍSICA E TIPO DE CONSTRUÇÃO

As operações de EC e ER da DigitalSign são conduzidas dentro de ambientes fisicamente protegidos que dissuadem, previnem e detetam o uso de acesso não autorizado ou a divulgação de informação sensível, quer seja encoberta ou evidente.

A DigitalSign também mantém instalações para a recuperação das suas operações EC em situações de catástrofe. As instalações da DigitalSign para recuperação em caso de catástrofe estão protegidas por múltiplos níveis de segurança física, comparável às instalações primárias da DigitalSign.

5.1.2. ACESSO FÍSICO

Os sistemas EC DIGITALSIGN estão protegidos por um mínimo de quatro níveis de segurança física hierárquicos, com requisitos de acesso o acesso ao nível inferior antes de ter acesso ao nível em questão.

Progressivamente, o acesso físico restritivo privilegia o controlo do acesso a cada nível. A atividade operacional sensível da EC, i.e., qualquer atividade relativa ao ciclo de vida do processo de certificação, tais como, autenticação, verificação e emissão, ocorrem dentro de níveis de acesso muito restritos. O acesso a cada nível requer o uso de um cartão de proximidade. O acesso físico é automaticamente autenticado e gravado em vídeo. Níveis adicionais obrigam ao acesso individual controlado através do uso de dois fatores de autenticação, incluindo biométrica. Pessoal sem escolta, incluindo funcionários não credenciados ou visitantes, não é permitido em tais áreas de segurança.

O sistema de segurança físico inclui níveis adicionais para a gestão de segurança de chaves, a qual serve para proteger o armazenamento online ou offline das Unidades de Assinatura Criptográfica (UAC) e material de suporte. As áreas usadas para criar e armazenar material criptográfico obrigam a um controlo duplo, cada um através do uso de dois fatores de autenticação, incluindo biometria. As UAC online estão protegidas através do uso de armários bloqueados. As UAC offline estão protegidas através do uso de cofres fechados, armários e contentores. O acesso às UAC e material de suporte é restrito, de acordo com a política de segregação de funções da DigitalSign. A abertura e fecho dos armários e recipientes nestes níveis são autenticados/registados para propósitos de auditorias.

5.1.3. ELETRICIDADE E AR CONDICIONADO

As instalações de segurança da DigitalSign estão equipadas com:

- Sistemas de eletricidade para assegurar acesso contínuo e ininterrupto de eletricidade.
- Sistemas de aquecimento/ventilação/ar condicionado para controlar a temperatura e humidade relativa.

5.1.4. EXPOSIÇÃO À ÁGUA

A DigitalSign tomou as devidas precauções para minimizar o impacto da exposição à água, incluindo detetores de inundação.

5.1.5. PREVENÇÃO E PROTEÇÃO CONTRA INCÊNDIOS

A DigitalSign tomou as devidas precauções para prevenir e extinguir incêndios ou outro tipo de exposição a chamas ou fumo que possam ser destruidoras. As medidas de prevenção e proteção de incêndios da DigitalSign foram concebidas para obedecer aos regulamentos de segurança local para incêndios.

5.1.6. SALVAGUARDA DE SUPORTES DE ARMAZENAMENTO

Todos os suportes que contenham software de produção e informação, auditoria, arquivo ou informação de apoio, são armazenados dentro das instalações com controlo de acesso físico e lógico apropriado, concebido para limitar acesso a pessoal autorizado e proteger tais suportes de informação de possíveis estragos acidentais (ex.: água, fogo e eletromagnético).

5.1.7. ELIMINAÇÃO DE RESÍDUOS

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

Suportes eletrónicos para recolha, armazenamento ou transmissão de dados sensíveis são formatados de forma segura ou destruídos fisicamente, de acordo com as instruções do fabricante.

Outros resíduos são tratados de acordo com as regras definidas internamente pela DigitalSign.

5.1.8. INSTALAÇÕES EXTERNAS PARA RECUPERAÇÃO DE SEGURANÇA

São efetuadas cópias de segurança de rotina de dados críticos e registos de auditoria. Todas as cópias de segurança em instalações externas são armazenadas em ambientes seguros.

5.2. CONTROLOS PROCESSUAIS

5.2.1. FUNÇÕES DE CONFIANÇA

Definem-se como Pessoas de Confiança todos os funcionários, colaboradores, contratados e consultores que tenham acesso ou controlem a autenticação ou operações de codificação, que possam afetar materialmente:

- A validação de informação dos pedidos de emissão de certificado.
- A aceitação, rejeição ou outros processos de subscrição de certificados, pedidos de revogação ou de renovação, ou informação de inscrição.
- A emissão ou revogação de certificados, incluindo pessoal que tenha acesso a porções restritas do repositório.
- O tratamento ou pedidos de informação do utilizador final.

Pessoas de Confiança inclui, mas não estão limitadas a:

- Pessoal do serviço de atendimento ao cliente.
- Pessoal de operações criptográficas.
- Pessoal de segurança.
- Pessoal de administração e operação de sistemas.

A DigitalSign considera as categorias de identificação de pessoal nesta secção como Pessoas de Confiança, possuindo Posições de Confiança. Pessoas que procuram tornar-se em Pessoas de Confiança obtendo uma Posição de Segurança, devem completar com sucesso os requisitos estabelecidos por esta DPC.

5.2.2. NÚMERO DE PESSOAS NECESSÁRIAS POR TAREFA

A DigitalSign estabeleceu e mantém uma política de controlo rigoroso de procedimentos, para garantir a segregação de poderes, baseada nas responsabilidades de cada tarefa, e assegurando que várias Pessoas de Confiança estão aptas a desempenhar tarefas sensíveis.

As políticas e procedimentos de controlo estão em vigor para garantir a segregação de deveres/funções baseada nas responsabilidades de cada tarefa. As tarefas mais delicadas, tais como o acesso e gestão do hardware criptográfico EC (unidade de assinatura criptográfica ou UAC) e material de suporte, requerem várias Pessoas de Confiança em simultâneo.

Estes procedimentos de controlo interno são designados para garantir no mínimo a necessidade de duas pessoas de confiança para acesso físico ou lógico ao dispositivo. O acesso ao hardware criptográfico EC é estritamente executado por várias Pessoas de Confiança, através do seu ciclo de vida, desde o momento de entrada e inspeção, à destruição lógica e/ou física. Uma vez ativo, um módulo com chaves operacionais, são invocados controlos de acesso adicionais, para manter a divisão do controlo sobre ambos os acessos físicos e lógicos ao dispositivo. Pessoas com acesso físico aos módulos, não detêm as chaves de ativação e vice-versa.

Outras operações manuais, tais como a validação e emissão de certificados qualificados, requerem a participação de pelo menos duas Pessoas de Confiança, ou a combinação de pelo menos uma Pessoa de Confiança e processo automatizado de validação e emissão.

5.2.3. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA CADA FUNÇÃO

Para todo o pessoal que pretende tornar-se numa Pessoa de Confiança, a verificação da identidade é desempenhada através de presença pessoal (física), perante as pessoas de confiança do Departamento de Recursos Humanos (ou equivalente). A identidade e outros requisitos do Estatuto de Pessoal de Confiança são posteriormente confirmados através de procedimentos de apoio para verificação, descritos nesta DPC.

A DigitalSign garante que ao pessoal que atingiu o Estatuto de Confiança, só posteriormente lhe foi concedido o acesso a:

- Dispositivos de controlo de acessos e acesso garantido às instalações.
- Credenciais eletrónicas para aceder e desempenhar funções específicas na EC, ER da DigitalSign, ou outros sistemas TI.

5.2.4. FUNÇÕES QUE NECESSITEM DE SEGREGAÇÃO DE PODERES

As funções que necessitem de separação de responsabilidades incluem, mas não estão limitados a:

- Validação de informação nos pedidos de emissão de certificados, pedidos de revogação ou de renovação, ou renovação de informação.
- Emissão ou revogação de certificados, incluindo pessoal com acesso a partes restritas do repositório.
- Manuseamento de informação ou pedidos do subscritor.
- Criação, emissão ou destruição de um Certificado EC.

5.3. CONTROLOS DO PESSOAL

Alguém que procure ser uma Pessoa de Confiança deve apresentar provas dos requisitos, qualificações e experiência necessária para desempenhar as suas possíveis tarefas de responsabilidade de forma competente e satisfatória. As verificações dos dados recolhidos são repetidas pelo menos de 10 em 10 anos, para pessoal que detenha Posições de Confiança.

5.3.1. REQUISITOS DE ANTECEDENTES, QUALIFICAÇÕES, EXPERIÊNCIA E CREDENCIAÇÃO

A DigitalSign requer que o pessoal que procure ser uma Pessoa de Confiança, apresente provas de antecedentes, qualificações, experiência e credenciação necessária para desempenhar as suas possíveis tarefas de responsabilidade, de forma competente e satisfatória.

5.3.2. PROCEDIMENTOS DE VERIFICAÇÃO DE ANTECEDENTES

Antes de conceder o estatuto de Pessoa de Confiança, a DigitalSign conduz verificações de antecedentes, as quais incluem mas não estão imitadas ao seguinte:

- Detenções por ofensas criminais ou penais associadas à natureza do emprego. Como exemplo, crimes envolvendo fraudes financeiras (i.e., desfalque, furto, roubo, desvio).
- Qualquer padrão de comportamento que indica irresponsabilidade pessoal, por exemplo:
    - Detenções por condução sobre efeito de álcool ou drogas.
    - Declarações de bancarrota.
    - Recentes problemas de crédito (até 3 anos) (i.e., hipotecas perdidas ou pagamentos do carro).
- Qualquer acrescento no currículo ou envolvendo aplicações profissionais:
    - Falsa declaração de emprego (i.e., reivindicar ter trabalhado para um empregador particular quando nunca o tenha feito).
    - Falsa declaração sobre as qualificações académicas (i.e., reivindicar ser possuidor de um grau académico sem nunca o ter obtido, ou inflacionar o nível do grau que realmente possui, tal como reivindicar ser possuidor de uma Licenciatura tendo somente obtido o grau de Bacharel).

Na medida em que quaisquer destes requisitos impostos por esta secção não sejam cumpridos devido a proibições ou limitações da lei local ou outras circunstâncias, a DigitalSign usará uma técnica de investigação substituta, permitida por lei, que forneça informação substancialmente semelhante, incluindo, mas não limitada à respetiva verificação dos antecedentes.

Fatores revelados na verificação de antecedentes que possam ser considerados passíveis de rejeição de candidatos para Posições de Confiança ou por desenvolver ações contra uma Pessoa de Confiança existente, normalmente incluem (mas não está limitada) ao seguinte:

- Apresentação falsa efetuada pelo candidato ou Pessoa de Confiança.
- Referências profissionais altamente desfavoráveis ou de pouca confiança
- Determinadas condenações criminais.
- Indicações de falta de responsabilidade financeira.

Relatórios que contenham tais informações são avaliados pelos recursos humanos e pessoal de segurança, que determina a ação apropriado, à luz do tipo, magnitude e frequência do comportamento descoberto pela verificação do seu passado. Tais ações podem incluir medidas que abranjam o cancelamento de ofertas de emprego efetuadas a candidatos para Posições de Confiança ou o fim da ocupação de Pessoas de Confiança já existentes.

O uso da informação revelada na verificação de antecedentes está sujeito à legislação local.

5.3.3. REQUISITOS DE INSTRUÇÃO

A DigitalSign fornece ao seu pessoal instrução após recrutamento, bem como os requisitos de instrução necessários para o desempenho das suas tarefas de forma competente e satisfatória. A DigitalSign mantém registos de tais instruções no seu Sistema de Gestão da Qualidade ISO 9001 (SGQ). A DigitalSign periodicamente revê e altera o seu programa de instrução, se necessário.

Os programas de instrução/cursos da DigitalSign são adaptados às responsabilidades individuais e incluem o seguinte:

- Conceitos básicos de Infraestruturas de Chaves Públicas
- Responsabilidades das funções
- Políticas operacionais e procedimentos de segurança
- Uso e operações de hardware e software implementados
- Relatório e manuseamento de incidentes
- Recuperação e procedimentos de continuação dos negócios em caso de catástrofe

5.3.4. FREQUÊNCIA E REQUISITOS DE INSTRUÇÃO DE RECICLAGEM

A DigitalSign fornece cursos de reciclagem e atualização ao seu pessoal, na medida e frequência requerida para garantir que o pessoal mantém níveis de proficiência requeridos para desempenhar as suas funções com responsabilidade, competência e satisfação. São fornecidos cursos de segurança periódicos de sensibilização, numa base regular.

5.3.5. FREQUÊNCIA E SEQUÊNCIA DE ROTAÇÃO NAS FUNÇÕES

Não estipulado.

5.3.6. SANÇÕES PARA AÇÕES NÃO AUTORIZADAS

Sanções disciplinares apropriadas são levadas a cabo devido a ações não autorizadas ou outras violações das políticas e procedimentos da DigitalSign. As sanções disciplinares podem incluir medidas como o fim do contrato e são proporcionais à frequência e severidade das ações não autorizadas.

5.3.7. REQUISITOS PARA PRESTADORES DE SERVIÇOS

Em situações excecionais, subcontratados ou consultores podem ser utilizados para ocupar posições de confiança. A esses subcontratados ou consultores serão exigidos os mesmos critérios de segurança que a um funcionário da DigitalSign em função equivalente.

Subcontratados e consultores independentes, que não tenham completado ou passado os procedimentos de verificação de antecedentes, especificado nesta DPC na secção 5.3.2, apenas têm acesso às instalações de segurança da DigitalSign, na medida em que sejam escoltados e diretamente supervisionados a todo o tempo por Pessoas de Confiança.

5.3.8. DOCUMENTAÇÃO FORNECIDA AO PESSOAL

A DigitalSign fornece aos seus funcionários e colaboradores a formação exigida e outros documentos necessários para desempenhar o seu trabalho com responsabilidade e competência.

5.4. PROCEDIMENTOS DE REGISTOS DE AUDITORIA

5.4.1. TIPO DE EVENTOS REGISTADOS

A DigitalSign, manual ou automaticamente, regista os seguintes tipos de eventos significativos:

- Gestão de eventos do ciclo de vida das chaves EC, incluindo:
    - Criação da chave, cópia de segurança, armazenamento, recuperação, arquivamento e destruição
    - Gestão de eventos do ciclo de vida dos dispositivos criptográficos
- Gestão de eventos do ciclo de vida dos certificados EC e utilizadores finais, incluindo:
    - Pedido de certificado, renovação e revogação
    - Processamento de pedidos com ou sem sucesso
    - Criação e emissão de certificados e LCR
- Eventos relativos à segurança, incluindo:
    - Tentativas de acesso ao sistema PKI, com ou sem sucesso
    - Ações na PKI e sistemas de segurança desempenhadas pelo pessoal da DigitalSign
    - Registos e ficheiros de segurança sensíveis lidos, escritos ou apagados
    - Alterações a perfis de segurança
    - Falhas de sistema e hardware e outras anomalias
    - Atividade das firewall e routers
    - Entrada e saída de visitantes nas instalações

O registo de entradas inclui os seguintes elementos:

- Data e hora de entrada
- Número de série ou de sequência da entrada, para entradas diárias automáticas
- Identidade da entidade que faz a entrada diária
- Tipo de entrada

O registo de auditoria para as ERs e Administradores de Gestão do serviço MPKI inclui:

- Tipo de documentos de identificação apresentados pelo candidato ao certificado
- Registo único de informação de identificação, números ou uma combinação dos mesmos (ex.: número da carta de condução do Candidato ao Certificado), ou documentos de identificação, se apropriado
- Local de armazenamento de cópias dos candidatos e documentos de identificação
- Identidade da entidade que aceita o pedido
- Método usado para a validação dos documentos de identificação, se existir
- Nome do recetor da EC ou da ER submetido, se apropriado

5.4.2. FREQUÊNCIA DA AUDITORIA DE REGISTOS

Registos são examinados, pelo menos, numa base semanal, para situações operacionais e de segurança significativas. Adicionalmente, a DigitalSign revê os seus registos de entrada, devido a atividades suspeitas ou pouco usuais, em resposta a alertas baseados em irregularidades e incidentes dentro do sistema EC e ER da DigitalSign.

O processamento de auditoria aos registos consiste numa revisão dos registos auditados e documentos para todas as situações significativas, num resumo de auditoria de registos. Revisões de registos incluem a verificação de que o registo não foi adulterado, através de uma inspeção a todos os registos de entrada e uma investigação a qualquer alerta ou irregularidade nos registos. Ações tomadas baseadas em revisões das entradas auditadas, também são documentadas.

5.4.3. PERÍODO DE RETENÇÃO DOS REGISTOS DE AUDITORIA

Os registos de auditoria são mantidos disponíveis até pelo menos dois meses após o processo e então arquivado de acordo com a secção 5.5.2.

5.4.4. PROTEÇÃO DOS REGISTOS DE AUDITORIA

A auditoria dos registos é protegida por controlo de acesso físico e lógico, que inclui mecanismos que protegem os ficheiros de registo, do visionamento não autorizado, modificações, supressões ou outro tipo de adulteração.

5.4.5. PROCEDIMENTOS PARA AS CÓPIAS DE SEGURANÇA DOS REGISTOS DE AUDITORIA

Cópias de segurança incrementais são criados diariamente e cópias completas são desempenhadas semanalmente.

5.4.6. SISTEMA DE RECOLHA DE REGISTOS
Os registos automáticos são gerados pelas próprias aplicações. Os registos manuais são gerados pelo pessoal da DigitalSign.

5.4.7. NOTIFICAÇÃO DE AGENTES CAUSADORES DE EVENTOS
Quando uma ocorrência é registada pelo sistema de recolha de auditorias, não é necessária qualquer notificação ao indivíduo, dispositivo ou candidato que provocou a mesma.

5.4.8. AVALIAÇÃO DE VULNERABILIDADES
Parte dos registos de auditoria são utilizados para monitorizar vulnerabilidades do sistema.

São desenvolvidas avaliações às vulnerabilidades da segurança lógica (AVSLs), bem como a sua revisão e análise.

As AVSLs são baseadas em registos automatizados e em tempo real, numa base diária, mensal e anual.

5.5. ARQUIVO DE REGISTOS

5.5.1. TIPO DE REGISTOS GUARDADOS
São arquivados, pelo menos:

- Todos os registos de auditoria recolhidos nos termos da secção 5.4
- Informação sobre o ciclo de vida dos certificados, incluindo pedidos e documentos de suporte

5.5.2. PERÍODO DE RETENÇÃO EM ARQUIVO
Os dados sujeitos a arquivo são retidos pelo período de tempo definido pela legislação aplicável, que atualmente se fixam em 20 (vinte) anos.

5.5.3. PROTEÇÃO DOS ARQUIVOS
A DigitalSign protege os seus registos arquivados, para que apenas Pessoas de Confiança autorizadas possam ter acesso ao mesmo. O arquivo é protegido contra visionamento não autorizado, modificações, supressão ou outras tentativas de adulteração, através do armazenamento em sistemas fidedignos. Os equipamentos que contêm a informação arquivada e as aplicações exigidas para o processo de arquivamento da informação, devem ser sujeitos a manutenção regular, para garantir que a informação do arquivo possa ser acedida durante o período estabelecido nesta DPC.

5.5.4. PROCEDIMENTOS PARA AS CÓPIAS DE SEGURANÇA DOS ARQUIVOS
Cópias de segurança incrementais são criados diariamente e cópias completas são desempenhadas semanalmente.

5.5.5. REQUISITOS PARA VALIDAÇÃO CRONOLÓGICA DOS REGISTOS
Algumas entradas contêm informações sobre a hora e a data. Tais informações não são geradas em equipamento criptográfico.

5.5.6. SISTEMA DE RECOLHA DE DADOS DE ARQUIVO (INTERNO OU EXTERNO)

O sistema de recolha de dados de arquivo é interno, exceto para clientes ER. A DigitalSign apoia os seus clientes ER na preservação dum registo de auditoria. Tal sistema de recolha de arquivo é, portanto, externo.

5.5.7. PROCEDIMENTOS PARA OBTENÇÃO E VERIFICAÇÃO DA INFORMAÇÃO DOS ARQUIVOS

Apenas Pessoas de Confiança autorizadas podem aceder ao arquivo. A integridade da informação é verificada quando é restaurada.

5.6. RENOVAÇÃO DE CHAVES

Nada a referir.

5.7. COMPROMETIMENTO E RECUPERAÇÃO EM CASO DE DESASTRE

5.7.1. PROCEDIMENTOS EM CASO DE INCIDENTES E COMPROMETIMENTO

Devem ser mantidas as seguintes cópias de segurança em instalações exteriores, e estarem disponíveis na eventualidade de um comprometimento ou catástrofe, incluindo dados aplicacionais de certificação, registos de auditoria e dados de todos os certificados emitidos.

As cópias de segurança da chave privada da EC devem ser criadas de acordo com a secção 6.2.4.

A DigitalSign manterá cópias de segurança dos dados necessários à operação da EC, bem como para a operação das ER.

5.7.2. CORRUPÇÃO DE RECURSOS INFORMÁTICOS, SOFTWARE E/OU DADOS

Na eventualidade de existir corrupção de recursos informáticos, software e/ou dados, tais ocorrências são relatadas à equipa de segurança da DigitalSign, e ativados os procedimentos aplicáveis. Esses procedimentos requerem escalamentos adequados, investigação e resposta ao mesmo. Se necessário, são ativados os procedimentos de comprometimento de chaves e ou de recuperação em caso de desastre.

5.7.3. PROCEDIMENTOS EM CASO DE COMPROMETIMENTO DA CHAVE PRIVADA DA EC

Perante a suspeita ou prova de comprometimento da chave privada da EC, serão tomadas as ações necessárias de resposta ao incidente.

Se for necessária a revogação do certificado EC, é posto é prática o procedimento seguinte:

- É comunicado às partes confiantes o estado de revogação do certificado, através do repositório, de acordo com esta DPC.
- São feitos esforços comerciais razoáveis, para fornecer notificação suplementar acerca da revogação a todos os participantes da STN afetados.

5.7.4. CAPACIDADE DE CONTINUAÇÃO DA ATIVIDADE APÓS DESASTRE

A DigitalSign dispõe de instalações secundárias redundantes, capazes de reativar as operações essenciais da EC DIGITALSIGN após desastre.

O plano de recuperação em caso de desastre é regularmente testado, verificado e atualizado, para que esteja operacional na eventualidade de qualquer ocorrência.

5.8. EXTINÇÃO DA EC OU ER

Na eventualidade de ser necessário cessar as operações da EC ou de qualquer uma das ER, a DigitalSign efetuará um esforço comercial razoável para notificar com antecedência os utilizadores finais, as partes confiantes e outras entidades afetadas por tal extinção.

Quando necessária a extinção da EC, a DigitalSign desenvolverá um plano de extinção para minimizar os efeitos aos seus clientes, utilizadores finais e partes confiantes. Tal plano deve conter o seguinte, conforme aplicável:

- Comunicar a cessação de atividade
- Comunicar a cessação da atividade à Autoridade Nacional de Segurança para efeitos do cancelamento das credenciações de segurança
- Cessar todas as relações contratuais com terceiros autorizados a atuarem em seu nome na execução de funções relativas à emissão de certificados
- Fornecer notificação às partes afetadas pelo termo, tais como, utilizadores finais, partes confiantes e clientes, informando-os do estado da EC
- Suportar os custos de tais notificações
- A revogação do certificado emitido à EC DIGITALSIGN
- A preservação do arquivo e registos da EC, durante o período imposto nesta DPC e legislação aplicável
- A continuação do auxílio de serviços a utilizadores finais e clientes
- A continuação de serviços de revogação, tais como a emissão da LCR e manutenção do serviço de verificação de estado online
- A revogação, se necessária, de todos os certificados emitidos que não estejam expirados ou já revogados
- Reembolsar, se necessário, os titulares dos certificados não expirados e não revogados, que sejam revogados sob o plano de extinção, ou alternativamente emitir certificados de substituição por uma EC sucessora
- Destruição (ou equivalente) da chave privada da EC e HSMs que as contêm
- Plano para a transição dos serviços EC para uma EC sucessora, garantindo que a entidade a quem é transmitida toda a documentação se obriga à sua manutenção durante o período de tempo legalmente exigido

6. CONTROLOS DE SEGURANÇA TÉCNICA

6.1. GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES

6.1.1. GERAÇÃO DO PAR DE CHAVES

A geração de chaves criptográficas da EC DIGITALSIGN é feita por elementos autorizados para tal, em nível 4 de segurança ou superior, numa cerimónia planeada e auditada de acordo com procedimentos escritos das operações a realizar, e utilizando sistemas que garantem os requisitos de força criptográfica das chaves. Todas as atividades desenvolvidas em cada cerimónia de geração de chaves ficam registadas, datadas e assinadas por todos os elementos envolvidos. Esses registos são mantidos para efeitos de auditoria futura.

O hardware criptográfico, usado para a geração de chaves da EC, cumpre pelo menos os requisitos FIPS 140-1 nível 3 e/ou Common Criteria EAL 4+.

As chaves para utilizadores finais são geradas em dispositivos qualificados de criação de assinatura, devidamente homologados.

6.1.2. ENTREGA DA CHAVE PRIVADA AO TITULAR

As chaves criptográficas relativas a um certificado qualificado usado para assinatura eletrónica avançada podem ser geradas remotamente num dispositivo qualificado de criação de assinatura, conforme requerido pelo Regulamento (EU) 910/2014. As chaves são geradas em dispositivos qualificados de criação de assinatura, devidamente aprovados. O controlo exclusivo de acesso à chave privada é garantido através do uso de dois fatores de autenticação.

Caso o par de chaves seja gerado pela ER em dispositivos seguros de criação de assinatura, a entrega do par de chaves e correspondente certificado é efetuada presencialmente ou através de correio postal registado ou equivalente. Os códigos de acesso ao dispositivo criptográfico são remetidos via correio eletrónico (para o endereço constante do certificado) após receção e verificação do "Termo de Receção", devidamente assinado pelo titular.

Se os signatários criarem as chaves em seu próprio dispositivo criptográfico, a DigitalSign verificará através do processo técnico ou uma declaração do auditor antes de emitir um certificado com as chaves criadas num dispositivo de hardware.

Todas as chaves são criadas usando o algoritmo de chave pública RSA, com um tamanho mínimo de 2048 bits.

O DigitalSign possui controlos para garantir que as chaves geradas estejam de acordo com as Políticas de Certificação, sob pena de não poder emitir os correspondentes certificados.

6.1.3. ENTREGA DA CHAVE PÚBLICA AO EMISSOR DO CERTIFICADO

Os utilizadores finais e ERs submetem as chaves públicas à EC DIGITALSIGN, para certificação eletrónica, através de pedido de emissão de certificado sob o formato PKCS#10.

6.1.4. ENTREGA DA CHAVE PÚBLICA DA EC A UTILIZADORES E PARTES CONFIANTES

A Digicert garante que os certificados EC raiz da STN são incluídos na esmagadora maioria dos web browsers, equipamentos e outros softwares existentes a nível global, incluindo em versões e atualizações.

Normalmente a DigitalSign fornece também toda a cadeia de certificados ao utilizador final, a ser incluída no dispositivo criptográfico disponibilizado.

Adicionalmente o certificado da EC DIGITALSIGN (e correspondente cadeia de certificação) pode ser obtido no diretório.

6.1.5. TAMANHO DAS CHAVES

O comprimento do par de chaves da EC DIGITALSIGN é 2048 bit RSA.

O comprimento mínimo do par de chaves para utilizadores finais é de 2048 bit RSA.

6.1.6. GERAÇÃO DE PARÂMETROS DA CHAVE PÚBLICA

Não aplicável.

6.1.7. UTILIZAÇÃO DA CHAVE (KEYUSAGE)

De acordo com o disposto na secção 7.1.2.1.

6.2. PROTEÇÃO DA CHAVE PRIVADA E CARACTERÍSTICAS DOS MÓDULOS CRIPTOGRÁFICOS

A DigitalSign implementou uma combinação de procedimentos de controlo físico e lógico para garantir a segurança da sua chave privada. Exige-se igualmente aos subscritores, através de contrato, que tomem as devidas precauções para prevenir perdas, divulgação, modificação ou uso não autorizado das suas chaves privadas.

6.2.1. NORMAS PARA MÓDULOS CRIPTOGRÁFICOS

Para a criação e armazenamento da chave privada da EC DIGITALSIGN são utilizados módulos de criptográficos de hardware, que são certificados ou reúnem materialmente os requisitos FIPS 140-1 Nível 3 e/ou Common Criteria EAL 4+.

6.2.2. CONTROLO MÚLTI-PESSOAL (M DE N) PARA A CHAVE PRIVADA

A DigitalSign implementou mecanismos técnicos e processuais que requerem a participação de vários funcionários de confiança para desempenhar operações criptográficas da EC. A DigitalSign usa a «partilha de segredos» para dividir a informação necessária para a ativação de uma chave privada em partes separadas, designadas por "segredos partilhados", os quais são detidos por indivíduos instruídos e de confiança, designados «Detentores de Chaves». O número limite de Partilhas de Segredo (m), de um número total de Detentores de Chave criados e distribuídos para um módulo criptográfico de hardware particular (n), é requerido para que se ative a chave privada EC armazenada no módulo.

As Partilhas de Segredos são protegidas de acordo com esta DPC na secção 6.4.2.

6.2.3. RETENÇÃO DA CHAVE PRIVADA (KEY ESCROW)

A retenção de chaves privadas não é usada pela DigitalSign.

O DigitalSign não armazena ou arquiva a chave privada de um Signatário destinada a criar assinatura/selo eletrónico, exceto no caso de certificação remota de um certificado qualificado através da solução de assinatura remota da DigitalSign.

Nesse caso, a chave privada é gerada num dispositivo qualificado de criação de assinatura (QSCD) e cifrada em um ambiente confiável. A cifra da chave é baseada numa chave simétrica AES (128 bits) criada pelo QSCD e derivada da *master wrapping key* do QSCD e

do primeiro fator de autenticação criado/definido pelo Signatário, o que garante que somente ele/ela possa aceder a essa chave em particular.

6.2.4. CÓPIA DE SEGURANÇA DA CHAVE PRIVADA

A DigitalSign faz backups de chaves privadas da CA para permitir a sua recuperação em caso de desastre natural, perda ou dano. Pelo menos duas pessoas são necessárias para criar a cópia e recuperá-la.

A DigitalSign mantém registros nos processos de gestão de chaves privadas da CA.

A DigitalSign não cria cópias das chaves privadas dos signatários, exceto no caso referido na seção anterior 6.2.3.

6.2.5. ARQUIVO DA CHAVE PRIVADA

Ver secção 6.2.3 e 4.1.2.

6.2.6. TRANSFERÊNCIA DA CHAVE PRIVADA DO/PARA O MÓDULO CRIPTOGRÁFICO

A DigitalSign cria pares de chaves diretamente no módulo criptográfico no qual são usadas.

A DigitalSign faz cópias dessas chaves com o propósito de recuperações rotineiras e em casos de desastres.

Quando as chaves são transferidas para outro módulo criptográfico (para efeitos de cópia de segurança), tais chaves são transferidas entre os módulos criptográficos de forma cifrada, e segundo as especificações do fabricante.

6.2.7. ARMAZENAMENTO DA CHAVE PRIVADA EM MÓDULO CRIPTOGRÁFICO

A chave privada da EC é guardada em módulo criptográfico na forma cifrada.

6.2.8. MÉTODO DE ATIVAÇÃO DA CHAVE PRIVADA

A chave privada da EC DIGITALSIGN é ativada conforme definido na secção 6.2.2. Depois da chave privada ser ativada, esta pode permanecer ativa por um tempo indefinido até ser desativada.

6.2.9. MÉTODO DE DESATIVAÇÃO DA CHAVE PRIVADA

A chave privada da EC DIGITALSIGN é desativada quando desligado o sistema da EC.

6.2.10. MÉTODO DE DESTRUIÇÃO DA CHAVE PRIVADA

Quando necessário, a DigitalSign poderá destruir a chave privada da EC, de forma a garantir que não existam *partes* da chave que possam levar à reconstrução da mesma. A DigitalSign garante a formatação (zeroisation) dos seus módulos criptográficos e outros meios apropriados para garantir a destruição completa de chaves. Quando realizadas, as atividades de destruição de chaves são registadas.

6.2.11. CLASSIFICAÇÃO DO MÓDULO CRIPTOGRÁFICO

Ver secção 6.2.1.

6.3. OUTROS ASPETOS DA GESTÃO DO PAR DE CHAVES

6.3.1. ARQUIVO DA CHAVE PÚBLICA

São feitas cópias de segurança e armazenados todos os certificados emitidos, como parte dos procedimentos de rotina da DigitalSign.

6.3.2. PERÍODOS DE UTILIZAÇÃO DE CHAVES PÚBLICAS E PRIVADAS

O período de utilização de um certificado termina aquando da expiração ou revogação do mesmo. O período de utilização do par de chaves é o mesmo que os definidos para os certificados associados, excetuando-se:

- As chaves privadas podem continuar a ser usadas para descodificação
- As chaves públicas podem continuar a ser usadas para verificação de assinaturas

O certificado da EC DIGITALSIGN tem um prazo de validade que pode variar dos cinco aos dez anos.

Os certificados de Validação Cronológica tem um prazo máximo de validade de seis anos.

Os certificados de utilizador final tem um prazo máximo de 40 meses.

Os certificados emitidos pela EC DIGITALSIGN têm um prazo de validade não superior ao do seu próprio certificado.

Além disso, EC DIGITALSIGN pode deixar de emitir novos certificados a partir de uma data apropriada, anterior à expiração do certificado EC, de tal forma que nenhum certificado emitido possa ter uma data de expiração posterior à data de expiração de qualquer um dos certificados constantes da cadeia de certificação.

6.4. DADOS DE ATIVAÇÃO

6.4.1. GERAÇÃO DE DADOS DE ATIVAÇÃO E INSTALAÇÃO

Os dados de ativação (Segredos Partilhados) usados, para proteção dos módulos criptográficos que contêm a chave privada da EC, são criados de acordo com os requisitos da secção 6.2.2 e com as especificações aplicáveis à cerimónia de criação de chaves. A criação e distribuição de segredos partilhados é devidamente registada.

A geração dos dados de ativação da chave privada dos signatários dependendo do tipo de certificado.

Nos smartcards ou usb tokens usados pela DigitalSign, as chaves são geradas protegidas com um PIN e PUK calculados aleatoriamente. Esta informação é enviada pela plataforma de gestão para o titular através do endereço de e-mail associado ao certificado digital. O titular possui software para alterar o PIN e o PUK do seu cartão.

Em dispositivos de hardware de terceiros, a DigitalSign acredita dispositivos de terceiros, embora sejam geridos separadamente.

As chaves privadas armazenadas num HSM para assinatura/selo remoto, os dados de ativação são criados/definidos pelo Signatário.

6.4.2. PROTEÇÃO DE DADOS DE ATIVAÇÃO

É requerido aos detentores dos Segredos Partilhados, que salvaguardem esses dados e assinem um acordo reconhecendo as suas responsabilidades.

Os dados de ativação são guardados em cofres seguros.

As chaves privadas de utilizador final são protegidas através da utilização de dispositivos seguros de criação de assinaturas e PIN (*Personal Identification Number*). No caso de utilização da solução de assinatura remota da DigitalSign, são requeridos dois fatores de autenticação.

6.4.3. OUTROS ASPETOS DE DADOS DE ATIVAÇÃO

6.4.3.1. TRANSMISSÃO DE DADOS DE ATIVAÇÃO

Sempre que seja necessário proceder à transmissão de dados de ativação, os mesmos devem ser protegidos contra perdas, roubo, modificações, visionamento ou uso não autorizado.

6.4.3.2. DESTRUIÇÃO DE DADOS DE ATIVAÇÃO

Os dados de ativação da chave privada da EC devem ser destruídos utilizando métodos que protejam contra perdas, roubo, modificação e visionamento e uso não autorizado das chaves privadas protegidas por tais dados de ativação. Após término do período de retenção em arquivo, secção 5.5.2, a DigitalSign deve destruir os dados de ativação, reescrevendo-os e/ou destruindo-os fisicamente.

6.5. CONTROLOS DE SEGURANÇA INFORMÁTICA

A DigitalSign desempenha todas as funções de EC e ER, utilizando sistemas fidedignos que reúnem os requisitos estipulados pela DigitalSign. A DigitalSign recomenda que os seus clientes de ER sigam as mesmas diretrizes.

6.5.1. REQUISITOS TÉCNICOS ESPECÍFICOS DE SEGURANÇA INFORMÁTICA

A DigitalSign garante que os sistemas de suporte às atividades da EC, são sistemas fidedignos e seguros contra acessos não autorizados. Além disso, a DigitalSign limita o acesso a servidores de produção apenas aos indivíduos que necessitam efetivamente desse acesso.

A rede de produção é logicamente separada de outras componentes. Esta separação previne o acesso à rede, exceto através de processos aplicacionais bem definidos. A DigitalSign usa sistemas de firewall para proteger a rede de intrusões internas ou externas, e limita a natureza e origem das atividades da rede que possam aceder a sistemas de produção.

6.5.2. CLASSIFICAÇÃO DA SEGURANÇA INFORMÁTICA

Não estipulado.

6.6. CONTROLOS TÉCNICOS DO CICLO DE VIDA

6.6.1. CONTROLOS DE DESENVOLVIMENTOS DE SISTEMAS

As aplicações são desenvolvidas e implementadas pela DigitalSign ou terceiros, de acordo com os sistemas de desenvolvimento e padrões de manutenção de alterações definidos. A DigitalSign também fornece software aos seus clientes para desempenhar funções de ER.

O software desenvolvido, quando carregado, fornece métodos para verificar se o software não foi alterado antes da instalação e é a versão correta para ser utilizada.

6.6.2. CONTROLOS DE GESTÃO DE SEGURANÇA

A DigitalSign dispõe de mecanismos e/ou políticas para controlar ou monitorizar a configuração da sua EC. Após a instalação e periodicamente, a DigitalSign avalia a integridade do seu sistema EC.

6.6.3. CLASSIFICAÇÃO DE SEGURANÇA DO CICLO DE VIDA

As operações de atualização e manutenção dos produtos e sistemas da EC seguem o mesmo controlo que o equipamento original e é instalado por pessoal autorizado e com adequada formação para o efeito, seguindo os procedimentos definidos.

6.7. CONTROLOS DE SEGURANÇA DA REDE

A DigitalSign desempenha todas as suas funções EC e ER usando redes seguras, para prevenir acessos não autorizados e outras atividades maliciosas. A DigitalSign protege a comunicação de informações sensíveis, através do uso de assinaturas digitais e cifra.

6.8. VALIDAÇÃO CRONOLÓGICA (TIME-STAMPING)

Certificados, LCR e outros dados de revogação contêm informação sobre a data e hora. Tal informação não é baseada em mecanismos criptográficos.

7. PERFIS DE CERTIFICADO E LCR

7.1. PERFIL DE CERTIFICADO

Os certificados emitidos pela EC DIGITALSIGN obedecem à norma *ITU-T Recomendation X.509 (1997): Information Technology – Open Systems Interconnection – The Directory: Authentication Framework*, e *RFC 3280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile*.

Os certificados emitidos contêm, pelo menos, os campos e valores descritos na tabela seguinte:

Campo	***Valor***
Número de Série (Serial Number)	Número de série único atribuído pela EC emissora
Algoritmo de Assinatura (Signature Algorithm)	Identificação do algoritmo utilizado para assinar os certificados (ver secção 7.1.3)
DN do Emissor (Issuer DN)	Ver secção 7.1.4
Data de Emissão (Valid From)	Indicação de data e hora em formato UTC, devidamente sincronizado através de Network Time Protocol, e codificado de acordo com o RFC 3280
Data de Expiração (Valid To)	Indicação de data e hora em formato UTC, devidamente sincronizado através de Network Time Protocol, e codificado de acordo com o RFC 3280
DN do Titular (Subject)	Ver secção 7.1.4
Chave Pública do Titular (Subject Public Key)	Codificada de acordo com o RFC 3280
Assinatura (Signature)	Assinatura do emissor, gerada e codificada de acordo com o RFC 3280

7.1.1. NÚMERO(S) DE VERSÃO

Tanto o certificado EC como todos os certificados emitidos pela mesma utilizam a versão 3 (três) do formato X.509.

7.1.2. EXTENSÕES DO CERTIFICADO

Os certificados contêm as extensões descritas nas secções 7.1.2.1 a 7.1.2.10.

7.1.2.1. KEY USAGE

Para certificados emitidos antes de 01/07/2016:

Campo	***EC***	***Certificados***	***Val.Cronológica***
Extensão crítica	*SIM*	*SIM*	*SIM*
Digital Signature (bit 0)	NÃO	SIM	SIM
Non Repudiation (bit 1)	NÃO	SIM	SIM
Key Encipherment (bit 2)	NÃO	NÃO	NÃO
Data Encipherment (bit 3)	NÃO	NÃO	NÃO
Key Agreement (bit 4)	NÃO	NÃO	NÃO
Key Certificate Signature (bit 5)	SIM	NÃO	NÃO
CRL Signature (bit 6)	SIM	NÃO	NÃO
Encipher Only (bit 7)	NÃO	NÃO	NÃO
Decipher Only (bit 8)	NÃO	NÃO	NÃO

Para certificados emitidos a partir de 01/07/2016:

Campo	EC	Certificados	Val.Cronológica
Extensão crítica	*SIM*	*SIM*	*SIM*
Digital Signature (bit 0)	NÃO	NÃO	SIM
Non Repudiation (bit 1)	NÃO	SIM	SIM
Key Encipherment (bit 2)	NÃO	NÃO	NÃO
Data Encipherment (bit 3)	NÃO	NÃO	NÃO
Key Agreement (bit 4)	NÃO	NÃO	NÃO
Key Certificate Signature (bit 5)	SIM	NÃO	NÃO
CRL Signature (bit 6)	SIM	NÃO	NÃO
Encipher Only (bit 7)	NÃO	NÃO	NÃO
Decipher Only (bit 8)	NÃO	NÃO	NÃO

7.1.2.2. CERTIFICATE POLICIES

Campo	EC	Certificados	Val.Cronológica
Extensão crítica	*NÃO*	*NÃO*	*NÃO*
Cert Policy ID	2.16.840.1.113733.1.7.23.2	2.16.840.1.113733.1.7.23.2	2.16.840.1.113733.1.7.23.2
Cert Policy Qualifier ID	1.3.6.1.5.5.7.2.1 (CPS Pointer)	1.3.6.1.5.5.7.2.1 (CPS Pointer)	1.3.6.1.5.5.7.2.1 (CPS Pointer)
Cert Qualifier	https://www.trustwise.com/cps	https://www.digitalsign.pt/ECDIGITALSIGN/cps	https://www.digitalsign.pt/ECDIGITALSIGN/cps
Cert Policy ID		--	
Cert Policy Qualifier ID	1.3.6.1.5.5.7.2.2 (User Notice)	--	--
Cert Qualifier	https://www.trustwise.com/rpa	--	--
Cert Policy ID	--	2.16.840.1.113733.1.7.44.2	--
Cert Policy ID	--	--	--
Cert Policy Qualifier ID	--	--	--
Cert Policy ID (1)	--	0.4.0.194112.1.2	--
Cert Policy ID	--	--	--
Cert Policy Qualifier ID	--	--	--
Cert Policy ID (2)	--	0.4.0.194112.1.3	--
Cert Policy ID	--	--	--
Cert Policy Qualifier ID	--	--	--

(1) Apenas presente nos certificados de perfil Individual, Membro, Profissional e Representação, emitidos pela EC DigitalSign Qualified CA – G3.

(2) Apenas presente nos certificados de perfil Organização, emitidos pela EC DigitalSign Qualified CA – G3.

7.1.2.3. SUBJECT ALTERNATIVE NAME

Campo	EC	Certificados	Val.Cronológica
Extensão crítica	*NÃO*	*NÃO*	--
	De acordo com o RFC 3280	RFC822 Name/email address	--

7.1.2.4. BASIC CONSTRAINTS

Campo	EC	Certificados	Val.Cronológica
Extensão crítica	*SIM*	*NÃO*	*SIM*
Subject Type	CA	End Entity	End Entity
Path Length Constraint	0	None	None

7.1.2.5. EXTENDED KEY USAGE

Campo	EC	Certificados	Val.Cronológica
Extensão crítica	--	*NÃO*	*SIM*

Server Authentication	--	NÃO	NÃO
Client Authentication	--	SIM	NÃO
Code Signing	--	NÃO	NÃO
Secure Email	--	SIM	NÃO
IPSEC End System	--	NÃO	NÃO
IPSEC Tunnel	--	NÃO	NÃO
IPSEC User	--	NÃO	NÃO
Time Stamping	--	NÃO	SIM
OCSP Signing	--	NÃO	NÃO
Microsoft Server Gated Crypto	--	NÃO	NÃO
Netscape SGC	--	NÃO	NÃO
Symantec SGC Identifier for CA Certificates	--	NÃO	NÃO

7.1.2.6. CRL DISTRIBUTION POINTS

Campo	*EC*	*Certificados*	*Val.Cronológica*
Extensão crítica	*NÃO*	*NÃO*	*NÃO*

7.1.2.7. AUTHORITY KEY IDENTIFIER

Esta extensão é preenchida com o *hash* da chave pública do emissor, através do algoritmo 160-bit SHA-1. Esta é uma extensão marcada como NÃO crítica.

7.1.2.8. SUBJECT KEY IDENTIFIER

Esta extensão é preenchida com o *hash* da chave pública do próprio certificado, através do algoritmo 160-bit SHA-1, ou segundo qualquer outro método descrito no RFC 3280. Esta é uma extensão marcada como NÃO crítica.

7.1.2.9. AUTHORITY INFORMATION ACCESS

Para certificados emitidos a partir de 01/07/2016, esta extensão inclui o URL onde pode ser encontrado o certificado da EC emissora do certificado. Esta é uma extensão marcada como NÃO crítica.

7.1.2.10. QUALIFIED CERTIFICATE STATEMENT

Os certificados emitidos pela EC DIGITALSIGN possuem a extensão "Qualified Certificate Statement" (OID 1.3.6.1.5.5.7.1.3), segundo o disposto no documento ETSI EN 319 412.

Esta é uma extensão marcada como NÃO crítica.

7.1.2.11. PRIVATE EXTENSIONS

Os certificados de utilizador final podem ainda ter uma extensão adicional – "Netscape Certificate Type" (OID 2.16.840.1.113730.1.1) – o qual possui o BIT 0 ativo (SSL Client).

O certificado EC pode inclui também esta extensão, possuindo a informação "SSL CA" e "S/MIME CA" ativas.

Esta é uma extensão marcada como NÃO crítica.

7.1.3. IDENTIFICADORES DE ALGORITMO

Os certificados são assinados com recurso ao algoritmo sha1WithRSAEncryption (OID 1.2.840.113549.1.1.5) ou sha256WithRSAEncryption (OID 1.2.840.113549.1.1.11).

7.1.4. FORMATO DOS NOMES

Os campos DN do Emissor (Issuer) e do Assunto (Subject) seguem o estipulado na secção 3.1.1.

Embora todos os campos descritos na secção 7.1.2 sejam comuns a todos os certificados emitidos a utilizadores finais, a DigitalSign subdivide os certificados que emite em 5 (cinco) tipos distintos (apelidados de "perfil"), cuja informação constante do DN do campo Assunto tem o significado descrito nas secções 7.1.4.1 a 7.1.4.5 seguintes.

7.1.4.1. PERFIL INDIVIDUAL

Este perfil de certificado tem como objetivo identificar uma pessoa singular.

Para certificados emitidos antes de 01/07/2016:

Tipo	*Obrigatório*	*Identificador*	*Descrição*
CN	SIM	--	Nome completo do titular
E	SIM	--	Endereço de email do titular, ou que o titular tem acesso
T	NÃO	--	Título académico ou outro que o titular possa utilizar
OU	NÃO	ID	Número de identificação, como por exemplo BI ou NIF
OU	NÃO	Address1	Endereço postal (linha 1)
OU	NÃO	Address2	Endereço postal (linha 2)
OU	NÃO	Postal Code	Código Postal
L	NÃO	--	Cidade ou Localidade
C	SIM	--	País
OU	NÃO	Limitation1	Eventuais limitações para utilização da assinatura (linha 1)
OU	NÃO	Limitation2	Eventuais limitações para utilização da assinatura (linha 2)
OU	NÃO	Limitation3	Eventuais limitações para utilização da assinatura (linha 3)
OU	NÃO	Obs1	Eventuais observações (linha 1)
OU	NÃO	Obs2	Eventuais observações (linha 2)
OU	NÃO	Obs3	Eventuais observações (linha 3)
OU	SIM	--	Terms of use at https://www.digitalsign.pt/ECDIGITALSIGN/rpa
OU	SIM	--	Certificate Profile - Qualified Certificate - Individual

Para certificados emitidos a partir de 01/07/2016:

Tipo	*Obrigatório*	*Identificador*	*Descrição*
CN	SIM	--	Nome completo do titular
OU	NÃO	RemoteQSCDManagement	Presente apenas nos certificados emitidos para assinatura remota
G	SIM	--	Primeiro(s) nome(s) do titular
SN	SIM	--	Apelido(s) do titular
SERIALNUMBER	NÃO	--	Número de identificação, conforme ETSI EN 319 412
E	SIM	--	Endereço de email do titular, ou que o titular tem acesso
C	SIM	--	País
OU	NÃO	Limitation1	Eventuais limitações para utilização da assinatura (linha 1)
OU	NÃO	Limitation2	Eventuais limitações para utilização da assinatura (linha 2)
OU	NÃO	Limitation3	Eventuais limitações para utilização da assinatura (linha 3)

OU	NÃO	Obs1	Eventuais observações (linha 1)
OU	NÃO	Obs2	Eventuais observações (linha 2)
OU	NÃO	Obs3	Eventuais observações (linha 3)
OU	SIM	--	Terms of use at https://www.digitalsign.pt/ECDIGITALSIGN/rpa
OU	SIM	--	Certificate Profile - Qualified Certificate - Individual

7.1.4.2. PERFIL PROFISSIONAL

Este perfil de certificado tem como objetivo identificar uma pessoa singular, e a sua titularidade no desempenho da sua profissão. Normalmente este tipo de certificado é emitido a membros de Ordens Profissionais, onde a titularidade deverá ser verificada junto dessa Ordem.

Para certificados emitidos antes de 01/07/2016:

Tipo	*Obrigatório*	*Identificador*	*Descrição*
CN	SIM	--	Nome completo do titular
E	SIM	--	Endereço de email do titular, ou que o titular tem acesso
T	NÃO	--	Título académico ou outro que o titular possa utilizar
OU	SIM	Entitlement	Título profissional verificado junto da Ordem Profissional
OU	NÃO	ID	Número de identificação, como por exemplo BI ou NIF
OU	NÃO	Address1	Endereço postal (linha 1)
OU	NÃO	Address2	Endereço postal (linha 2)
OU	NÃO	Postal Code	Código Postal
L	NÃO	--	Cidade ou Localidade
C	SIM	--	País
OU	NÃO	Limitation1	Eventuais limitações para utilização da assinatura (linha 1)
OU	NÃO	Limitation2	Eventuais limitações para utilização da assinatura (linha 2)
OU	NÃO	Limitation3	Eventuais limitações para utilização da assinatura (linha 3)
OU	NÃO	Obs1	Eventuais observações (linha 1)
OU	NÃO	Obs2	Eventuais observações (linha 2)
OU	NÃO	Obs3	Eventuais observações (linha 3)
OU	SIM	--	Terms of use at https://www.digitalsign.pt/ECDIGITALSIGN/rpa
OU	SIM	--	Certificate Profile - Qualified Certificate - Professional

Para certificados emitidos a partir de 01/07/2016:

Tipo	*Obrigatório*	*Identificador*	*Descrição*
CN	SIM	--	Nome completo do titular
OU	NÃO	RemoteQSCDManagement	Presente apenas nos certificados emitidos para assinatura remota
G	SIM	--	Primeiro(s) nome(s) do titular
SN	SIM	--	Apelido(s) do titular
SERIALNUMBER	NÃO	--	Número de identificação, conforme ETSI EN 319 412
E	SIM	--	Endereço de email do titular, ou que o titular tem acesso
OU	SIM	Entitlement	Título profissional verificado junto da Ordem Profissional

C	SIM	--	País
OU	NÃO	Limitation1	Eventuais limitações para utilização da assinatura (linha 1)
OU	NÃO	Limitation2	Eventuais limitações para utilização da assinatura (linha 2)
OU	NÃO	Limitation3	Eventuais limitações para utilização da assinatura (linha 3)
OU	NÃO	Obs1	Eventuais observações (linha 1)
OU	NÃO	Obs2	Eventuais observações (linha 2)
OU	NÃO	Obs3	Eventuais observações (linha 3)
OU	SIM	--	Terms of use at https://www.digitalsign.pt/ECDIGITALSIGN/rpa
OU	SIM	--	Certificate Profile - Qualified Certificate - Professional

7.1.4.3. PERFIL MEMBRO

Este perfil de certificado tem como objetivo identificar uma pessoa singular, e o cargo ou função que ocupa/desempenha numa determinada organização.

Para certificados emitidos antes de 01/07/2016:

Tipo	*Obrigatório*	*Identificador*	*Descrição*
CN	SIM	--	Nome completo do titular
E	SIM	--	Endereço de email do titular, ou que o titular tem acesso
T	NÃO	--	Título académico ou outro que o titular possa utilizar
OU	SIM	Entitlement	Cargo ou função que ocupa/desempenha na organização (ver campo "O")
OU	NÃO	ID	Número de identificação, como por exemplo BI ou NIF
OU	NÃO	Address1	Endereço postal
OU	NÃO	Postal Code	Código Postal
L	NÃO	--	Cidade ou Localidade
C	SIM	--	País
O	SIM	--	Nome completo da organização onde ocupa/desempenha o cargo ou função definida no campo "OU = Entitlement"
OU	NÃO	Organization ID	Identificador da organização, como por exemplo o NIPC
OU	NÃO	Organization Address1	Endereço postal da organização
OU	NÃO	Organization PostalCode	Código Postal da organização
OU	NÃO	Organzation City	Cidade ou Localidade da organização
OU	NÃO	Organization Limitation1	Eventuais limitações para utilização da assinatura (linha 1)
OU	NÃO	Organization Limitation2	Eventuais limitações para utilização da assinatura (linha 2)
OU	NÃO	Organization Limitation3	Eventuais limitações para utilização da assinatura (linha 3)
OU	NÃO	Obs1	Eventuais observações
OU	SIM	--	Terms of use at https://www.digitalsign.pt/ECDIGITALSIGN/rpa
OU	SIM	--	Certificate Profile - Qualified Certificate - Member

Para certificados emitidos a partir de 01/07/2016:

Tipo	*Obrigatório*	*Identificador*	*Descrição*
CN	SIM	--	Nome completo do titular

OU	NÃO	RemoteQSCDManagement	Presente apenas nos certificados emitidos para assinatura remota
G	SIM	--	Primeiro(s) nome(s) do titular
SN	SIM	--	Apelido(s) do titular
SERIALNUMBER	NÃO	--	Número de identificação, conforme ETSI EN 319 412
E	SIM	--	Endereço de email do titular, ou que o titular tem acesso
T	NÃO	--	Título académico ou outro que o titular possa utilizar
OU	SIM	Entitlement	Cargo ou função que ocupa/desempenha na organização (ver campo "O")
C	SIM	--	País
O	SIM	--	Nome completo da organização onde ocupa/desempenha o cargo ou função definida no campo "OU = Entitlement"
ORGANIZATION IDENTIFIER	SIM	--	Número de identificação da organização, conforme ETSI EN 319 412
OU	NÃO	Limitation1	Eventuais limitações para utilização da assinatura (linha 1)
OU	NÃO	Limitation2	Eventuais limitações para utilização da assinatura (linha 2)
OU	NÃO	Limitation3	Eventuais limitações para utilização da assinatura (linha 3)
OU	NÃO	Obs1	Eventuais observações (linha 1)
OU	NÃO	Obs2	Eventuais observações (linha 2)
OU	NÃO	Obs3	Eventuais observações (linha 3)
OU	SIM	--	Terms of use at https://www.digitalsign.pt/ECDIGITALSIGN/rpa
OU	SIM	--	Certificate Profile - Qualified Certificate - Member

7.1.4.4. PERFIL ORGANIZAÇÃO

Este perfil de certificado tem como objetivo identificar uma pessoa coletiva.

Trata-se de um certificado de selo eletrónico que se destina exclusivamente a ser usado por uma pessoa coletiva.

Não é uma figura idónea para vincular contratualmente a pessoa coletiva, da mesma forma que no mundo físico um carimbo/selo de uma organização não é suficiente para vincular a mesma.

Tipo	*Obrigatório*	*Identificador*	*Descrição*
CN	SIM	--	Nome completo do titular (organização)
OU	NÃO	RemoteQSCDManagement	Presente apenas nos certificados emitidos para assinatura remota
E	SIM	--	Endereço de email do titular, ou que o titular tem acesso
C	SIM	--	País
O	SIM	--	Nome completo da organização
ORGANIZATION IDENTIFIER	SIM	--	Número de identificação da organização, conforme ETSI EN 319 412
OU	NÃO	Limitation1	Eventuais limitações para utilização do selo (linha 1)
OU	NÃO	Limitation2	Eventuais limitações para utilização do selo (linha 2)
OU	NÃO	Limitation3	Eventuais limitações para utilização do selo (linha 3)
OU	NÃO	Obs1	Eventuais observações (linha 1)
OU	NÃO	Obs2	Eventuais observações (linha 2)
OU	NÃO	Obs3	Eventuais observações (linha 3)
OU	SIM	--	Terms of use at https://www.digitalsign.pt/ECDIGITALSIGN/rpa

OU	SIM	--	Certificate Profile - Qualified Certificate - Organization

7.1.4.5. PERFIL REPRESENTAÇÃO

Este perfil de certificado tem como objetivo identificar uma pessoa singular, como legal representante ou procurador de uma organização, com poderes para obrigar sozinho uma pessoa coletiva, com eventuais limitações identificadas nos respetivos campos do certificado.

Para certificados emitidos antes de 01/07/2016:

Tipo	*Obrigatório*	*Identificador*	*Descrição*
CN	SIM	--	Nome completo da organização
E	SIM	--	Endereço de email do representante, ou que o representante tem acesso
OU	SIM	Entitlement	Poderes de representação que o representante/procurador detêm
C	SIM	--	País
OU	NÃO	ID	Identificador da organização, como por exemplo o NIPC
OU	NÃO	Address1	Endereço postal da organização (linha 1)
OU	NÃO	Address2	Endereço postal da organização (linha 2)
OU	NÃO	PostalCode	Código Postal da organização
OU	NÃO	City	Cidade ou Localidade da organização
OU	SIM	Representative Name	Nome completo do representante/procurador
OU	NÃO	Representative ID	Número de identificação do representante/procurador, como por exemplo BI ou NIF
OU	NÃO	Representative Limitations1	Eventuais limitações para utilização da assinatura por parte do representante/procurador (linha 1)
OU	NÃO	Representative Limitations2	Eventuais limitações para utilização da assinatura por parte do representante/procurador (linha 2)
OU	NÃO	Representative Limitations3	Eventuais limitações para utilização da assinatura por parte do representante/procurador (linha 3)
OU	NÃO	Obs1	Eventuais observações (linha 1)
OU	NÃO	Obs2	Eventuais observações (linha 2)
OU	NÃO	Obs3	Eventuais observações (linha 3)
OU	SIM	--	Terms of use at https://www.digitalsign.pt/ECDIGITALSIGN/rpa
OU	SIM	--	Certificate Profile - Qualified Certificate - Representative

Para certificados emitidos a partir de 01/07/2016:

Tipo	*Obrigatório*	*Identificador*	*Descrição*
CN	SIM	--	Nome completo do titular
OU	NÃO	RemoteQSCDManagement	Presente apenas nos certificados emitidos para assinatura remota
G	SIM	--	Primeiro(s) nome(s) do titular
SN	SIM	--	Apelido(s) do titular
SERIALNUMBER	NÃO	--	Número de identificação, conforme ETSI EN 319 412
E	SIM	--	Endereço de email do titular, ou que o titular tem acesso
T	NÃO	--	Título académico ou outro que o titular possa utilizar
OU	SIM	Entitlement	Poderes de representação que o representante/procurador (titular) detêm
C	SIM	--	País

O	SIM	--	Nome completo da organização
ORGANIZATION IDENTIFIER	SIM	--	Número de identificação da organização, conforme ETSI EN 319 412
OU	NÃO	Limitations1	Eventuais limitações para utilização da assinatura por parte do representante/procurador (linha 1)
OU	NÃO	Limitations2	Eventuais limitações para utilização da assinatura por parte do representante/procurador (linha 2)
OU	NÃO	Limitations3	Eventuais limitações para utilização da assinatura por parte do representante/procurador (linha 3)
OU	NÃO	Obs1	Eventuais observações (linha 1)
OU	NÃO	Obs2	Eventuais observações (linha 2)
OU	NÃO	Obs3	Eventuais observações (linha 3)
OU	SIM	--	Terms of use at https://www.digitalsign.pt/ECDIGITALSIGN/rpa
OU	SIM	--	Certificate Profile - Qualified Certificate - Representative

7.1.5. RESTRIÇÕES AOS NOMES
Não estipulado.

7.1.6. IDENTIFICADOR DA POLÍTICA DE CERTIFICADOS
Onde utilizada esta extensão, os certificados contêm o respetivo identificador conforme estabelecido na CP da STN, secção 1.2.

7.1.7. UTILIZAÇÃO DA EXTENSÃO POLICY CONSTRAINTS
Não estipulado.

7.1.8. SINTAXE E SEMÂNTICA DOS POLICY QUALIFIERS
Os certificados contêm um "Policy Qualifier" na extensão "Certificate Policies", conforme descrito na secção 7.1.2.2.

7.1.9. SEMÂNTICA DE PROCESSAMENTO PARA A EXTENSÃO CRÍTICA CERTIFICATE POLICY
Não estipulado.

7.2. PERFIL DE LCR

As LCR emitidas contêm os campos básicos e conteúdos específicos na tabela seguinte:

Campo	*Valor*
Versão	Ver secção 7.2.1
Algoritmo de Assinatura (Signature Algorithm)	Identificação do algoritmo utilizado para assinar as LCR. O algoritmo utilizado é sha1WithRSAEncryption (OID 1.2.840.113549.1.1.5)
Emissor (Issuer)	Entidade emissora da LCR
Data Efectiva (Efective Date)	Data de emissão da LCR. As LCR são efetivas após emissão.
Próxima Actualização (Next Update)	Data em que a próxima LCR será emitida. A frequência de emissão das LCR é definida na secção 4.4.7
Certificados Revogados (Revoked Certificates)	Lista dos certificados revogados, incluindo o número de série e a data de revogação.

7.2.1. NÚMERO(S) DE VERSÃO

É utilizada a versão 2 (dois) do formato X.509 para LCR, conforme RFC 3280.

7.2.2. EXTENSÕES DA LCR

Não estipulada.

7.3. PERFIL DE OCSP

O protocolo OSCP (Online Status Certificate Protocol) é uma forma de a DigitalSign dar informação acerca do estado de revogação de um certificado em particular.

Os OCSP Responders estão conforme o disposto no RFC 2560.

7.3.1. NÚMERO(S) DE VERSÃO

É utilizada a versão 1 (um) da especificação OCSP, conforme RFC 2560.

7.3.2. EXTENSÕES DO OCSP

A DigitalSign não utiliza o "*nonce*" nas respostas OCSP.

8. AUDITORIAS E AVALIAÇÕES DE CONFORMIDADE

É desempenhada uma auditoria anual por entidade acreditada para o Centro de Operações de Dados e Operações de Manutenção de Chave da DigitalSign/BT, que apoiam os serviços de gestão da EC DIGITALSIGN.

Além das avaliações de conformidade e auditorias, a DigitalSign é responsável por desempenhar outras revisões e investigações, para garantir a fidedignidade do subdomínio que opera na STN, o que inclui, mas não se limita ao seguinte:

- A DigitalSign, ou o seu representante autorizado, é responsável, dentro do seu único e exclusivo critério, por desempenhar, a qualquer momento, uma auditoria ou investigação a um cliente ER, na eventualidade de haver motivos para crer que a entidade auditada tenha falhado no cumprimento dos padrões da STN, tenha sofrido um incidente, tenha agido ou não agiu para que a entidade não falhasse, o que pode potencialmente ameaçar a segurança ou integridade da STN.
- A DigitalSign, ou o seu representante autorizado, é responsável por avaliar a Gestão de Risco a clientes ER, no cumprimento normal das suas tarefas.

A DigitalSign, ou os seus representantes legais, podem delegar a realização destas auditorias, avaliações ou investigações a uma terceira parte auditora devidamente acreditada pelas entidades competentes. Entidades que estejam sujeitas a auditorias, avaliações ou investigações devem estabelecer cooperação com a DigitalSign e com o pessoal que realize a auditoria, avaliação ou investigação.

8.1. FREQUÊNCIA E CIRCUNSTÂNCIAS DAS AUDITORIAS

As auditorias são realizadas, pelo menos, numa base anual.

8.2. IDENTIDADE/QUALIFICAÇÕES DO AUDITOR

As auditorias às EC DIGITALSIGN devem ser realizadas por auditor devidamente credenciado, nos termos da legislação local aplicável.

8.3. RELAÇÃO ENTRE O AUDITOR E A ENTIDADE AUDITADA

As operações de auditoria à DigitalSign são realizadas por auditor independente.

8.4. ÂMBITO DA AUDITORIA

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

8.5. AÇÕES DESENVOLVIDAS COMO RESULTADO DE DEFICIÊNCIAS

Com respeito aos resultados das avaliações de conformidade ou auditorias, as exceções ou deficiências significativas identificadas resultarão na determinação das ações a serem desenvolvidas.

Esta determinação é feita pela administração da DigitalSign, em conjunto com os responsáveis das áreas em causa. A administração da DigitalSign é responsável pelo desenvolvimento e execução do plano de ação corretivo. Se DigitalSign determinar que tais

exceções ou deficiências possam constituir uma ameaça imediata à segurança ou à integridade da STN, esse plano deverá ser desenvolvido num prazo máximo de 30 dias e executada dentro de um período de tempo comercialmente razoável. Para exceções ou deficiências menos graves, a administração da DigitalSign avaliará as implicações de tais ocorrências e determinará o curso de ação apropriado.

8.6. COMUNICAÇÃO DE RESULTADOS

Os resultados das auditorias e avaliações de conformidade devem ser entregues à DigitalSign dentro dos prazos estipulados contratualmente.

A informação sobre as ações corretivas efetuadas e/ou a efetuar deverão ser remetidas à entidade competente no mais curto espaço de tempo possível (quando aplicável).

9. OUTROS ASSUNTOS DE CARÁCTER COMERCIAL E LEGAL

9.1. HONORÁRIOS

9.1.1. HONORÁRIOS POR EMISSÃO OU RENOVAÇÃO DE CERTIFICADOS

Poderão ser cobrados honorários pelos processos de emissão, e/ou Renovação de certificados.

9.1.2. HONORÁRIOS PARA ACESSO AOS CERTIFICADOS

Não são cobrados quaisquer honorários pela disponibilização dos certificados em repositório.

9.1.3. HONORÁRIOS PARA ACESSO À INFORMAÇÃO DE ESTADO OU REVOGAÇÃO DE CERTIFICADOS

Não são cobrados quaisquer honorários pela disponibilização das LCR em repositório, de acordo com o estipulado nesta DPC.

A emissão de LCR customizadas, serviços OCSP, ou qualquer outro serviço de valor acrescentado sobre informação de estado ou revogação de certificados estará sujeita à cobrança dos honorários contratualizados.

9.1.4. HONORÁRIOS DE OUTROS SERVIÇOS

A consulta desta DPC e demais documentos relativos a políticas, práticas e procedimentos não está sujeita a qualquer cobrança de honorários.

Devem ser garantidos os direitos de propriedade destas informações.

9.1.5. POLÍTICA DE REEMBOLSO

Não estão previstos reembolsos por qualquer ação de revogação de certificados.

9.2. RESPONSABILIDADE FINANCEIRA

9.2.1. COBERTURA DO SEGURO

A DigitalSign mantém uma cobertura de seguro para eventuais erros e omissões praticados no âmbito da sua atividade, através de seguro de responsabilidade civil com um capital fixado em lei de 125.000 €.

9.2.2. OUTROS RECURSOS

Os clientes ER devem dispor de recursos financeiros suficientes para manter as suas operações e desempenhar os seus deveres, devem suportar os riscos de responsabilidade aos seus subscritores e partes confiantes.

9.3. CONFIDENCIALIDADE DA INFORMAÇÃO

9.3.1. ÂMBITO DA CONFIDENCIALIDADE DA INFORMAÇÃO

Os seguintes registos de devem ser mantidos confidenciais e privados, segundo a secção 9.3.2:

- Registo dos pedidos de emissão de certificados
- Chave privada da EC DIGITALSIGN, e demais elementos de segurança a si inerentes
- Registos transacionais (ambos os registos completos e o rastreio de)
- Qualquer informação relativa a parâmetros de segurança
- Relatórios de auditorias realizadas pela DigitalSign ou os seus auditores (quer sejam internos ou externos)
- Planos de contingência ou de recuperação de falhas
- Medidas de segurança de controlo das operações do hardware e software da DigitalSign e de administração de serviços de certificação.

9.3.2. INFORMAÇÃO FORA DO ÂMBITO DA CONFIDENCIALIDADE DA INFORMAÇÃO

Informação sobre certificados, revogação e outra sobre o estado de certificados, o repositório da DigitalSign e informação nele contida não são considerados Informação Confidencial/Privada.

Informação que não seja expressamente considerada Informação Confidencial/Privada, ao abrigo da secção 9.3.1, não deve ser considerada confidencial nem privada. Esta secção está sujeita a leis de privacidade aplicáveis.

9.3.3. RESPONSABILIDADES DE PROTEÇÃO DA CONFIDENCIALIDADE DA INFORMAÇÃO

A DigitalSign garante a segurança de informação confidencial, evitando que possa ser desvendada ou comprometida por terceiras partes.

9.4. PRIVACIDADE DA INFORMAÇÃO PESSOAL

9.4.1. PLANO DE GARANTIA DE PRIVACIDADE

A DigitalSign mantém em repositório a sua Política de Privacidade.

9.4.2. INFORMAÇÃO PRIVADA

Qualquer informação acerca dos subscritores que não esteja publicamente disponível através do conteúdo dos certificados emitidos, diretório de certificados e LCR, é tratada como privada.

9.4.3. INFORMAÇÃO CONSIDERADA NÃO-PRIVADA

Sujeita a legislação eventualmente aplicável, toda a informação tornada publica num certificado não é considerada privada.

9.4.4. RESPONSABILIDADES DE PROTEÇÃO DA INFORMAÇÃO PRIVADA

Todos os participantes da STN que recebam informação privada devem evitar que seja comprometida ou desvendada a terceiras partes, e deve cumprir com todas as leis de privacidade aplicáveis.

9.4.5. NOTIFICAÇÃO E CONSENTIMENTO DE UTILIZAÇÃO DA INFORMAÇÃO PRIVADA

A menos que estabelecido de outra forma nesta DPC, na Politica de Privacidade aplicável ou contratualmente, a informação privada não será usada sem o consentimento da parte a quem a informação se aplica. Esta secção está sujeita à aplicação de leis de privacidade.

9.4.6. DIVULGAÇÃO POR IMPOSIÇÃO DA JUSTIÇA

Todos os participantes do subdomínio da DigitalSign devem reconhecer que a DigitalSign é forçada a desvendar Informação Confidencial/Privada se, de boa-fé, a DigitalSign considerar necessária a sua divulgação como resposta a intimações e mandatos judiciais.

9.4.7. OUTRAS CIRCUNSTÂNCIAS PARA DIVULGAÇÃO

Não estipuladas.

9.5. DIREITOS DE PROPRIEDADE INTELECTUAL

A atribuição de direitos de propriedade intelectual entre os participantes do subdomínio da STN, que não os utilizadores finais e partes confiantes, é determinado pelos contratos aplicáveis a esses participantes.

Todos os direitos de propriedade intelectual, incluindo certificados, LCR, OIDs, DPC e par de chaves da EC pertencem aos seus legítimos detentores/autores/emissores.

Os pares de chaves dos titulares dos certificados são propriedade dos mesmos, bem como dos nomes e demais informação constante do DN.

9.6. REPRESENTAÇÕES E GARANTIAS

9.6.1. REPRESENTAÇÕES E GARANTIAS DA EC

A DigitalSign garante:

- Que não há deturpações materiais de factos no certificado, conhecidos ou originários das entidades que aprovam a emissão dos certificados ou que emitem os certificados.
- Que não existem erros na informação do certificado, que tenham sido introduzidos pelas entidades que os aprovam ou emitem, como resultado de uma falha no exercício das suas funções.
- Que os certificados emitidos reúnem todos os requisitos desta DPC.
- O serviço de revogação e utilização do repositório, conforme esta DPC, em todos os aspetos materiais.

9.6.2. REPRESENTAÇÕES E GARANTIAS DA ER

Os contratos da DigitalSign com ERs garantem:

- Que não há deturpações materiais de factos no certificado, conhecidos ou originários das entidades que aprovam a emissão dos certificados ou que emitem os certificados.
- Que não existem erros na informação do certificado, que tenham sido introduzidos pelas entidades que os aprovam ou emitem, como resultado de uma falha no exercício das suas funções.
- Que os certificados emitidos reúnem todos os requisitos desta DPC.
- O serviço de revogação e utilização do repositório, conforme esta DPC, em todos os aspetos materiais.

9.6.3. REPRESENTAÇÕES E GARANTIAS DOS TITULARES

Os contratos da DigitalSign com os titulares dos certificados garantem que:

- Aceitam e obrigam-se a cumprir o contrato de emissão de certificado digital
- Obrigam-se a respeitar as regras de utilização do certificado digital (e respetiva chave privada) e garantem que não modificarão, por qualquer forma, a sua configuração técnica
- Garantem a confidencialidade do processo de obtenção e de utilização do certificado digital e respetiva chave privada
- Declaram que sabem quais são os efeitos legais atribuídos ao uso do certificado digital e assinatura digital
- Declaram que se responsabilizam por todo e qualquer uso que seja dado ao certificado digital (e correspondente chave privada) e pelas consequências que dele decorram
- Declaram que se obrigam a revogar online ou a informar por escrito, de imediato, a DigitalSign em caso de suspeita ou perda de controlo da chave privada ou de incorreção ou alteração da informação constante do certificado, enquanto for válido
- Declaram que a partir da revogação do certificado ou do termo do seu prazo de validade, é proibida a utilização dos respetivos dados de criação de assinatura para gerar uma assinatura eletrónica.

9.6.4. REPRESENTAÇÕES E GARANTIAS DAS PARTES CONFIANTES

As obrigações de terceiras partes confiantes que reconheçam que têm informação suficiente para tomar uma decisão informada, na medida em que escolham confiar na informação que consta num certificado, pelo que são os únicos responsáveis por decidir se confiar ou não em tais informações, e suportarão as consequências legais, caso falhem no desempenho das obrigações de parte confiante desta DPC.

9.7. RENÚNCIA DE GARANTIAS

A DigitalSign recusa todas as garantias que não se encontrem vinculadas nas obrigações estabelecidas nesta DPC.

9.8. LIMITAÇÕES DE RESPONSABILIDADE DA EC

A DigitalSign garante os danos ou prejuízos causados aos utilizadores finais e partes confiantes decorrentes da sua atividade, conforme legislação aplicável.

A DigitalSign não se responsabiliza por qualquer dano ou prejuízo decorrente utilizações abusivas ou fora do âmbito do contrato estabelecido com os utilizadores e/ou partes confiantes.

A DigitalSign não assume qualquer responsabilidade em caso falha dos serviços relacionada com causas de força maior, como desastres naturais, guerra ou outros similares.

9.9. INDEMNIZAÇÕES

A DigitalSign assumirá a sua responsabilidade no tocante a eventuais indemnizações, de acordo com a legislação aplicável.

9.10. TERMO E CESSAÇÃO

9.10.1. TERMO

Todos os documentos relacionados com a atividade da EC, incluindo esta DPC, e quaisquer alterações subsequentes, tornam-se efetivos após publicação no repositório.

9.10.2. CESSAÇÃO

Todos os documentos relacionados com a atividade da EC, incluindo esta DPC, e quaisquer alterações subsequentes, permanecerão ativos até publicação de nova versão ou alteração.

9.11. NOTIFICAÇÕES INDIVIDUAIS E COMUNICAÇÕES

A menos que seja especificado de outra forma, através de um acordo entre as partes, os participantes do subdomínio da DigitalSign devem usar métodos de comunicação entre si, comercialmente razoáveis, considerando a credibilidade e delicadeza da comunicação.

9.12. ALTERAÇÕES

9.12.1. PROCEDIMENTO PARA ALTERAÇÕES

Para garantir a atualização desta DPC, a administração da DigitalSign reúne, com uma periodicidade máxima de 1 (um) ano, com a Direção de Operações e com os Serviços Técnicos para avaliação das eventuais necessidades de melhoria e alteração.

As alterações a esta DPC devem ser aprovadas pela administração. As alterações devem ser efetuadas através de documentos, contendo a forma alterada da DPC ou por uma atualização.

As alterações, correções e/ou atualizações deverão ser publicadas sob a forma de novas versões desta DPC (e/ou respetivas PCs), substituindo qualquer versão anterior.

9.12.2. MECANISMOS E PRAZOS DE NOTIFICAÇÃO

A DigitalSign reserva o direito de corrigir estas DPC sem notificação prévia para correções que não sejam materialmente relevantes de acordo com o critério da DigitalSign, incluindo mas não limitado a erros escrita, mudanças URLS, mudanças de contactos, etc.

Em casos em que as alterações ou retificações possam afetar a aceitabilidade dos certificados para os fins que foram emitidos, tentar-se-á, de forma comercialmente aceitável, a notificação aos interessados de que foi efetuada a alteração ou retificação.

9.12.3. MOTIVOS PARA ALTERAÇÃO DE IDENTIFICADOR

Se a DigitalSign determinar que a alteração ao identificador (OID) da política de certificados é necessária, a alteração deve conter os novos identificadores. De outra forma, as alterações não devem requerer uma mudança no identificador da política de certificados.

9.13. DISPOSIÇÕES PARA RESOLUÇÃO DE CONFLITOS

9.13.1. RESOLUÇÃO DE CONFLITOS ENTRE A DIGITALSIGN E CLIENTES ER

Estes conflitos devem ser resolvidos mediante as disposições do contrato estabelecido entre as partes.

9.13.2. RESOLUÇÃO DE CONFLITOS COM OS UTILIZADORES OU PARTES CONFIANTES

Mediante o que é permitido por lei, todos os contratos devem conter uma cláusula para resolução de conflitos.

9.14. LEI VIGENTE

Sujeita a quaisquer limites impostos por lei, a Lei Portuguesa deve exercer a autoridade, construção, interpretação e validade desta DPC, independentemente do contrato ou outra escolha de disposição legal. Esta escolha da lei é feita para garantir procedimentos e interpretações uniformes a todos os participantes do subdomínio que a DigitalSign opera na STN, não interessando a sua localização.

9.15. CONFORMIDADE COM A LEI VIGENTE

Esta DPC está sujeito às leis, regras, regulações, ordenações, decretos, ou outros, sejam eles nacionais, estatais, locais ou estrangeiros, incluindo, mas não limitada, a restrições na importação ou exportação de software, hardware ou informação técnica.

9.16. PROVIDÊNCIAS VÁRIAS

9.16.1. ACORDO COMPLETO

Não aplicável.

9.16.2. INDEPENDÊNCIA

Não aplicável.

9.16.3. SEVERIDADE

Não aplicável.

9.16.4. EXECUÇÕES

Não aplicável.

9.16.5. FORÇA MAIOR

Não aplicável.

9.17. OUTRAS PROVIDÊNCIAS

9.17.1. GRUPO DE GESTÃO

O Grupo de Gestão é constituído por:

- Administrador
- Diretor Geral
- Diretor da Qualidade
- Administrador de Sistemas
- Operador de Sistemas
- Administrador de Segurança
- Auditor de Sistemas
- Consultor Externo (por convite)

As atribuições, objetivos e responsabilidades, deste grupo de gestão estão definidas em documentos internos da EC.

10. APÊNDICE A – ACRÓNIMOS E DEFINIÇÕES

EC	Entidade Certificadora
EC DIGITALSIGN	Entidade Certificadora da DigitalSign – Certificadora Digital, SA
DPC	Declaração de Práticas de Certificação
CP	Symantec Trust Network Certificate Policies
STN	Symantec Trust Network - hierarquia de confiança da Symantec
PKI	Infraestrutura de Chaves Públicas
OID	Número único de "identificador de objeto"
BT	British Telecomunications, plc
Symantec	Symantec, Inc
ER	Entidade de Registo
LCR	Lista de Certificados Revogados
OCSP	Online Status Certificate Protocol
PC	Políticas de Certificados
UAC	Unidades de Assinatura Criptográfica
AVSL	Avaliação às Vulnerabilidades da Segurança Lógica
FIPS	United State Federal Information Processing Standards
HSM	Hardware Security Module
PKCS	Public-Key Cryptography Standard
RFC	Request for comment
S/MIME	Secure multipurpose Internet mail extensions
SSL	Secure Sockets Layer