SISP – SOCIEDADE INTERBANCÁRIA E SISTEMAS DE PAGAMENTO

Declaração de Práticas de Certificação da Entidade de Certificação Raiz da SISP

- DPC da SISP-Root CA -

Cód.	PLRC001.05
Versão:	5.0
Data da versão:	30/06/2019
Criado por:	SISP
Aprovado por:	Direção Geral
Nível de confidencialidade:	Público

Histórico de alterações

Data	Versão	Criado por	Descrição da alteração
Janeiro de 2018	1.0	SISP	Criação do documento
Março de 2018	2.0	SISP	Actualização do documento
13/04/2018	3.0	SISP	Actualização do modelo de documento
31/07/2018	4.0	SISP	Alteração da estrutura hierárquica da PKI da SISP
30/06/2019	5.0	SISP	Disponibilização do certificado de autenticação web

Documentos relacionados

Politica de Certificados SISP Root CA

Índice

1. INTRODUÇÃO

1.1. OBJECTIVOS

O objectivo deste documento é definir os procedimentos e práticas utilizadas pela Entidade de Certificação Raiz da SISP (SISP Root CA) no suporte à sua actividade de certificação digital.

1.2. PÚBLICO-ALVO

Este documento é público e destina-se a todos quantos se relacionam com a Entidade de Certificação Raiz da SISP doravante designada de SISP Root CA, em particular aos Auditores e Colaboradores da SISP.

1.3. ESTRUTURA DO DOCUMENTO

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

O ponto 2 apresenta um conjunto de acrónimos e definições úteis para a leitura do documento. Os dez seguintes, são dedicados aos procedimentos e práticas mais importantes no âmbito da certificação digital da Entidade de Certificação Raiz da SISP. O décimo terceiro ponto é reservado a matérias legais.

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

2. ACRÓNIMOS E DEFINIÇÕES

2.1. ACRÓNIMOS

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

2.2 DEFINIÇÕES

Assinatura digital, conforme disposto no DL-nº33/2007, de 24 de Setembro	Modalidade de assinatura electrónica avançada baseada em sistema criptográfico assimétrico composto de um algoritmo ou série de algoritmos, mediante o qual é gerado um par de chaves assimétricas exclusivas e interdependentes, uma das quais privada e outra pública, e que permite ao titular usar a chave privada para declarar a autoria do documento electrónico ao qual a assinatura é aposta e concordância com o seu conteúdo e ao destinatário usar a chave pública para verificar se a assinatura foi criada mediante o uso da correspondente chave privada e se o documento electrónico foi alterado depois de aposta a assinatura.
Assinatura electrónica, conforme disposto no DL-nº33/2007, de 24 de Setembro	Dados sob forma electrónica anexos ou logicamente associados a uma mensagem de dados e que sirvam de método de autenticação.
Assinatura electrónica avançada, conforme disposto no DL-nº33/2007, de 24 de Setembro.	Assinatura electrónica que preenche os seguintes requisitos: i) Identifica de forma unívoca o titular como autor do documento; ii) A sua aposição ao documento depende apenas da vontade do titular; iii) É criada com meios que o titular pode manter sob seu controlo exclusivo; iv) A sua conexão com o documento permite detectar toda e qualquer alteração superveniente do conteúdo deste.
Assinatura electrónica qualificada, conforme disposto no DL-nº33/2007, de 24 de Setembro.	Assinatura digital ou outra modalidade de assinatura electrónica avançada que satisfaça exigências de segurança idênticas às da assinatura digital baseadas num certificado qualificado e criadas através de um dispositivo seguro de criação de assinatura.
Autoridade credenciadora, conforme disposto no DL-nº33/2007, de 24 de Setembro.	Entidade competente para a credenciação e fiscalização das Entidades de Certificação.
Certificado, conforme disposto no DL- nº33/2007, de 24 de Setembro	Documento electrónico que liga os dados de verificação de assinatura ao seu titular e confirma a identidade desse titular.
Certificado qualificado, conforme disposto no DL-nº33/2007, de 24 de Setembro	Certificado que contém os elementos referidos no artigo 67.º do DL 33/2007 [6] e é emitido por entidade de certificação que reúne os requisitos definidos no artigo 45.º do DL 33/2007.
Chave privada, conforme disposto no DL- nº33/2007, de	Elemento do par de chaves assimétricas destinado a ser

24 de Setembro	conhecido apenas pelo seu titular, mediante o qual se apõe a assinatura digital no documento electrónico, ou se decifra um documento electrónico previamente cifrado com a Correspondente chave pública.
Chave pública, conforme disposto no DL- nº33/2007, de 24 de Setembro	Elemento do par de chaves assimétricas destinado a ser divulgado, com o qual se verifica a assinatura digital aposta no documento electrónico pelo titular do par de chaves assimétricas, ou se cifra um documento electrónico a transmitir ao titular do mesmo par de chaves.
Credenciação, conforme disposto no DL- nº33/2007, de 24 de Setembro	Acto pelo qual é reconhecido a uma entidade, que o solicite e que exerça a actividade de entidade de certificação, o preenchimento dos requisitos definidos no DL-nº33/2007, de 24 de Setembro para os efeitos nele, previstos.
Dados de criação de assinatura, conforme disposto no DL-nº33/2007, de 24 de Setembro	Um conjunto único de dados, como códigos ou chaves criptográficas privadas, usado pelo signatário para a criação de uma assinatura electrónica.
Dados de verificação de assinatura, conforme disposto no DL-nº33/2007, de 24 de Setembro	Um conjunto de dados, como códigos ou chaves criptográficas públicas, usado para verificar a assinatura electrónica.
Dispositivo de criação de assinatura, conforme disposto no DL-nº33/2007, de 24 de Setembro	Suporte lógico ou dispositivo de equipamento utilizado para possibilitar o tratamento dos dados de criação de assinatura.
Dispositivo seguro de criação de assinatura, conforme disposto no DL-nº33/2007, de 24 de Setembro	Dispositivo de criação de assinatura que assegure, através de meios técnicos e processuais adequados, que, i) Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura só possam ocorrer uma única vez e que a confidencialidade desses dados se encontre assegurada; ii) Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura não possam, com um grau razoável de segurança, ser deduzidos de outros dados e que a assinatura esteja protegida contra falsificações realizadas através das tecnologias disponíveis; iii) Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura possam ser eficazmente protegidos pelo titular contra a utilização ilegítima por terceiros; iv) Os dados que careçam de assinatura não sejam modificados e possam ser apresentados ao titular antes do processo de assinatura.
Documento electrónico, conforme disposto no DL-nº33/2007, de 24 de Setembro.	Documento elaborado mediante processamento electrónico de dados.
Endereço electrónico, conforme disposto no DL-nº33/2007, de 24 de Setembro.	Identificação de um equipamento informático adequado para receber e arquivar documentos electrónicos.

3. CONTEXTO GERAL

3.1. OBJECTIVO

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

Este documento descreve as práticas gerais de emissão e gestão de certificados, seguidas pela SISP Root CA, explica o que um certificado fornece e significa, assim como os procedimentos que deverão ser seguidos por Partes Confiantes e por qualquer outra pessoa interessada para confiarem nos Certificados emitidos pela SISP Root CA.

Este documento pode sofrer actualizações regulares.

Os certificados emitidos pela SISP Root CA contêm uma referência à presente DPC, Codigo documento nº PLRC001.03, de modo a permitir que Partes confiantes e outras pessoas interessadas, possam encontrar informação sobre o certificado e sobre a entidade que o emitiu.

3.2. ENQUADRAMENTO

As práticas de criação, assinatura e de emissão de Certificados, assim como de revogação de certificados, cujo prazo de validade foi ultrapassado ou a pedido do titular, levadas a cabo por uma EC são fundamentais para garantir a fiabilidade e confiança de uma Infraestrutura de Chaves Publicas.

Esta DPC aplica-se especificamente à SISP ROOT CA, de acordo com a estrutura em uso no âmbito da ICP-CV e com os seguintes standards:

a) RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework;
b) RFC 5280 - Internet X.509 PKI - Certificate and CRL Profile.

e especifica, como implementar os procedimentos e controlos usados na SISP ROOT CA, e como a SISP ROOT CA deve atingir os requisitos especificados nas normas da ICP-CV.

3. 3. IDENTIFICAÇÃO DO DOCUMENTO

Este documento é uma DPC que é representada num certificado através de um número único designado de “identificador de objecto” (OID), sendo o valor do OID associado a este documento, o 2.16.132.1.1.2.3.

Este documento é identificado pelos dados constantes na seguinte tabela:

INFORMAÇÃO DO DOCUMENTO	
Versão do Documento	Versão 5.0
Estado do Documento	Aprovado
OID	2.16.132.1.1.2.3
Data de Emissão	30/06/2018
Validade	Não aplicável
Localização	https://pki.sisp.cv/

3.4. PARTICIPANTES NA INFRA-ESTRUTURA DE CHAVE PÚBLICA

A SISP, enquanto Entidade Gestora da PKI da SISP, cumpre as disposições previstas nas normas e legislação aplicável, assumindo as competências aí descritas sendo responsável por fornecer serviços e assegurar os procedimentos que possam garantir as funcionalidades a seguir indicadas:

1. Geração dos pares de chaves criptográficas associadas a cada uma das Entidades Certificadoras;

2. Receção e validação dos pedidos de emissão de certificados realizados pelas Entidades de Certificação (EC`s) subordinadas bem como os demais subscritores;

3. Emissão de certificados, relativos a pedidos de certificados que estejam de acordo com o formato requerido pelas Entidades de Certificação da SISP;

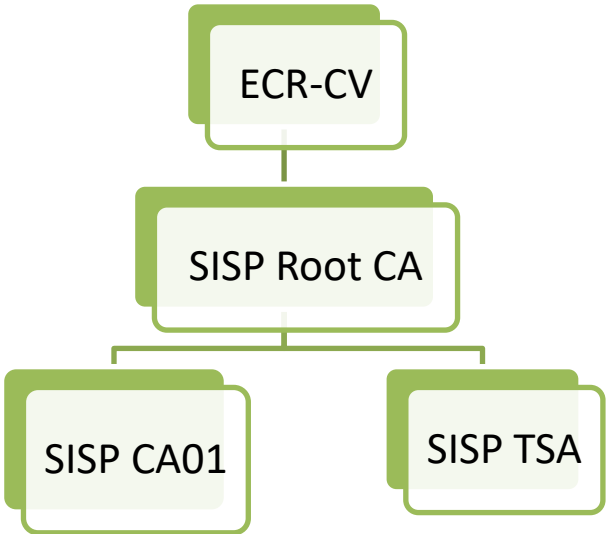
4. Receção e validação dos pedidos de suspensão e revogação de certificados;

5. Publicação dos certificados (quando, onde e se apropriado) e de informação acerca do seu estado;

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

A PKI da SISP é composta pelas seguintes EC's:

- Entidade Certificadora de Raiz de Cabo Verde (ECR-CV)
- SISP Root Certification Authority (SISP Root CA)
- SISP Certification Authority (SISP CA01)
- SISP TimeStamp Certification Authority (SISP TSA)



3.4.1. SISP ROOT CERTIFICATION AUTHORITY (SISP ROOT CA)

A SISP Root CA insere-se na hierarquia de confiança da ICP-CV, constituindo-se numa entidade de certificação de segundo nível assinada pela Entidade Certificadora de Raiz de Cabo Verde (ECR-CV), estando habilitada apenas a emitir certificados para assinar os certificados das ECs de nível hierárquico imediatamente inferior, conforme lista publicada em http://pki.sisp.cv.

3.4.2. SISPCA01 CERTIFICATION AUTHORITY (SISP CA01)

A Entidade Certificadora Subordinada SISP CA01 constitui uma Entidade Certificadora credenciada pela ARME – Agência Multisectorial de Regulação Económica, conforme a legislação caboverdiana, estando habilitadas, legalmente a emitir todo o tipo de certificado, incluindo certificados qualificados, os de mais elevado grau de segurança previsto na lei.

Encontra-se inserida na hierarquia de confiança da Infraestrtautura de Chaves Publicas de Cabo Verde.

A SISPCA01 pode emitir certificados de,

- Assinatura Qualificada para pessoa singular
- Assinatura Qualificada para representação da pessoa colectiva
- Assinatura Qualificada de Qualidade (Ordens Profissionais)
- Autenticação para pessoa singular e colectiva
- Autenticação WEB
- Selo electronico

bem como Validação Online OSCP.

3.4.3. SISP TSA ENTIDADE CERTIFICADORA DE VALIDAÇÃO CRONOLOGICA OU TIMESTAMP

A SISP TSA - Entidade Certificadora de Validação Cronologica é uma EC que emite certificados digitais integrantes da heirarquia de confiança da SISP e que pode igualmente, emitir selos temporais para outras finalidades em que se mostre necessario o comprovativo da hora legal.

A hora legal utilizada na validação cronologica é obtida utilizandoum cluster de equipamentos com relógio atomico, dedicado, com cobertura de 12 satelites e nivel de imprecisão de rede entre 1-10 millisegundos e GPS inferior a 1 microsegundo, com referência a UTC.

3.4.4. ENTIDADES OU UNIDADES DE REGISTO

Entidades ou Unidades de Registo são entidades às quais as ECs delegam a prestação de serviços de identificação, registo de utilizadores de certificados, bem como a gestão de pedidos de renovação e revogação de certificados. A SISP poderá actuar como Unidade de Registo e/ou estabelecer acordos com entidades terceiras para que estas desempenham este papel. A lista da Entidades Registo integrantes da PKI da SISP encontra-se publicada em em http://pki.sisp.cv.

3.4.5.TITULARES DE CERTIFICADOS

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

b) O titular do certificado da SISP ROOT CA é a SISP.

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

3.4.6. PATROCINADOR

Nada a assinalar

3.4.7. PARTES CONFIANTES

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

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

3.4.8.OUTROS PARTICIPANTES

3.4.8.1. AUTORIDADE CREDENCIADORA

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

Assim, consideram-se como principais atribuições as seguintes:

a) Acreditar as entidades de certificação;

b) Controlar as entidades de certificação;

c) Cobrar taxas pelos serviços de acreditação;

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

e) Auditar as entidades de certificação;

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

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

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

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

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

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

l) O mais que lhe for cometido por lei.

3.4.8.2. AUDITOR DE SEGURANÇA

Figura independente do círculo de influência da Entidade de Certificação, exigida pela Autoridade Credenciadora. A sua missão é auditar a infraestrutura da Entidade de Certificação, no que respeita a equipamentos, recursos humanos, processos, políticas e regras, tendo que submeter um relatório anual, à Autoridade Credenciadora. A lista de Auditores de Segurança de Entidades Certificadoras credenciados pela Entidade Credenciadora pode ser encontrada em http://www.pki.ecrcv.cv/.

3.5. UTILIZAÇÃO DO CERTIFICADO

3.5.1. CERTIFICADOS EMITIDOS

Os certificados emitidos pela SISP Root CA são exclusivos para a assinatura de certificados digitais das Entidades Certificação de nivel imediatamente subsequente ao seu, de sua Lista de Certificados Revogados (CRL) e da SISP TSA , com o objectivo de garantir os seguintes serviços:

- Controlo de acessos;
- Confidencialidade;
- Intergridade;
- Auntenticação e
- Não-repudio.

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

3.5.2. UTILIZAÇÃO ADEQUADA

Os requisitos e regras definidos neste documento aplicam-se a todos os certificados emitidos pela SISP Root CA.

Os certificados emitidos pela SISP Root CA são também utilizados pelas partes confiantes para verificação da cadeia de confiança de um certificado emitido sob a ICP-CV, assim como para garantir a autenticidade e identidade do emissor de uma assinatura digital gerada pela chave privada correspondente à chave pública contida num certificado assinado pela PKI da SISP.

Os certificados emitidos pela SISP Root CA devem ser utilizados de acordo com a função e finalidade estabelecida neste documento, nas correspondentes Políticas de Certificados e de acordo com a legislação em vigor.

3.5.3. UTILIZAÇÃO NÃO AUTORIZADA

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

Os certificados emitidos pela PKI da SISP não poderão ser utilizados para qualquer função fora do âmbito das utilizações descritas anteriormente.

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

3.6. GESTÃO DAS POLÍTICAS

A gestão desta DPC é da responsabilidade do Grupo de Trabalho Segurança, que pode ser contactada pelos telefones e no seguinte endereço:

Nome:	Grupo de Trabalho de Segurança
Morada:	SISP, SA Conj. Habitacional Novo Horizonte, Rua Cidade de Funchal, Achada Santo Antonio – Praia, Cabo Verde
Correio electrónico:	pki@sisp.cv
Site:	www.sisp.cv
Telefone:	2606310/2626317

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

A validação desta DPC (e/ou respetivas PCs) e seguintes correções (ou atualizações) deverão ser levadas a cabo pelo Grupo de Trabalho de Segurança. Correções (ou atualizações) deverão ser publicadas sob a forma de novas versões desta DPC (e/ou respetivas PCs), substituindo qualquer DPC (e/ou respetivas PCs) anteriormente definida.

O Grupo de Trabalho de Segurança deverá ainda determinar quando é que as alterações na DPC (e/ou respetivas PCs) levam a uma alteração nos identificadores dos objetos (OID) da DPC (e/ou respetivas PCs).

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

Todas as políticas, regras e praticas de certificação implementadas no ambito desta DPC podem ser consultadas no repositorio disponivel em http://pki.sisp.cv.

4. DISPOSIÇÕES LEGAIS

4.1 OBRIGAÇÕES E GARANTIAS

4.1.1 OBRIGAÇÕES E GARANTIAS DAS ENTIDADES CERTIFICADORAS

A PKI da SISP está obrigada a:

- Realizar as suas operações de acordo com esta Política;
- Declarar de forma clara todas as suas Práticas de Certificação no documento apropriado,
- Proteger as suas chaves privadas;
- Emitir certificados de acordo com o standard X.509;
- Emitir certificados que estejam conformes com a informação conhecida no momento de sua emissão e livres de erros de entrada de dados;
- Garantir a confidencialidade no processo da geração dos dados da criação da assinatura e a sua entrega por um procedimento seguro ao titular;
- Utilizar sistemas e produtos fiáveis que estejam protegidos contra toda a alteração e que garantam a segurança técnica e criptográfica dos processos de certificação;
- Utilizar sistemas fiáveis para armazenar certificados reconhecidos que permitam comprovar a sua autenticidade e impedir que pessoas não autorizadas alterem os dados;
- Arquivar sem alteração os certificados emitidos;
- Garantir que podem determinar com precisão da data e hora em que emitiu ou extinguiu ou suspendeu um certificado;
- Empregar pessoal com qualificações, conhecimentos e experiência necessárias para a prestação de serviços de certificação;
- Revogar os certificados nos termos da secção 7.7 deste documento e publicar os certificados revogados na CRL do repositório da SISP Root CA, com a frequência estipulada na secção 7.7.10;
- Publicar a sua DPC e as Políticas de Certificado aplicáveis no seu repositório garantindo o acesso às versões atuais assim como as versões anteriores;
- Notificar com a rapidez necessária, por correio eletrónico os titulares dos certificados em caso da EC proceder à revogação ou suspensão dos mesmos, indicando o motivo que originou esta ação;
- Colaborar com as auditorias dirigidas pela Autoridade Credenciadora, para validar a renovação das suas próprias chaves;
- Operar de acordo com a legislação aplicável;
- Proteger em caso de existirem as chaves que estejam sobre sua custódia;
- Garantir a disponibilidade da CRL de acordo com as disposições da secção 7.7.10;
- Em caso de cessar a sua atividade deverá comunicar com uma antecedência mínima de três meses a todos os titulares dos certificados emitidos assim como à Autoridade Credenciadora;
- Cumprir com as especificações contidas na norma sobre Proteção de Dados Pessoais;
- Conservar toda a informação e documentação relativa a um certificado reconhecido e as Declarações de Práticas de Certificação vigentes em cada momento e durante vinte anos desde o momento da emissão e,
- Disponibilizar os certificados da SISP Root CA.

4.1.2 OBRIGAÇÕES E GARANTIAS DAS ENTIDADES DE REGISTO

Nada a assinalar.

4.1.3 OBRIGAÇÕES E GARANTIAS DOS TITULARES

É obrigação dos titulares dos certificados emitidos:

- Limitar e adequar a utilização dos certificados de acordo com as utilizações previstas nas Politicas de Certificado;
- Tomar todos os cuidados e medidas necessárias para garantir a posse da sua chave privada;
- Solicitar de imediato a revogação de um certificado em caso de ter conhecimento ou suspeita de compromisso da chave privada correspondente à chave pública contida no certificado, de acordo com a secção 7.7.5;
- Não utilizar um certificado digital que tenha perdido a sua eficácia, quer por ter sido revogado, suspendido ou por ter expirado o período de validade;
- Submeter às Entidade de Certificação (ou de Registo) a informação que considerem exata e completa com relação aos dados que estas solicitem para realizar o processo de registo. Deve informar a EC de qualquer modificação desta informação e,
- Não monitorizar, manipular ou efetuar ações de "engenharia inversa" sobre a implantação técnica (hardware e software) dos serviços de certificação, sem a devida autorização prévia, por escrito, da PKI da SISP.

4.1.4 OBRIGAÇÕES E GARANTIAS DAS PARTES CONFIANTES

É obrigação das partes que confiem nos certificados emitidos pela PKI da SISP:

- Limitar a fiabilidade dos certificados às utilizações permitidas para os mesmos em conformidade com o expresso na Politica de Certificado correspondente;
- Verificar a validade dos certificados no momento de realizar qualquer operação baseada nos mesmos;
- Assumir a responsabilidade na correta verificação das assinaturas digitais;
- Assumir a responsabilidade na comprovação da validade, revogação ou suspensão dos certificados em que confia;
- Ter pleno conhecimento das garantias e responsabilidades aplicáveis na aceitação e uso de certificados em que confia e aceitar sujeitar-se às mesmas.

4.1.5 OBRIGAÇÕES E GARANTIAS DE OUTROS PARTICIPANTES

Nada a assinalar.

4.2 RESPONSABILIDADES DE PUBLICAÇÃO E ARMAZENAMENTO

A SISP reserva o direito de publicar informação relativa a certificados digitais emitidos por esta, num repositório disponível online, assim como de publicar informação sobre o estado do certificado em repositórios de terceiras partes.

A SISP mantém um repositório de documentos online onde divulga informação sobre as suas práticas, procedimentos e conteúdo de determinadas políticas, incluindo a DPC. Todas as partes associadas à emissão,

utilização ou gestão de certificados da SISP são aqui notificadas de que a mesma pode publicar informação submetida, no seu repositório acessível publicamente, no sentido de disponibilizar informação sobre o estado do certificado digital.

A SISP abstém-se de disponibilizar publicamente informação confidencial, designadamente a relacionada com controlos de segurança, procedimentos, políticas de segurança internas, entre outros.

4.2.1 REPOSITÓRIOS

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

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

- A CRL e DPC só podem ser alterados através de processos e procedimentos bem definidos,
- A Plataforma tecnológica do repositório encontra-se devidamente protegida pelas técnicas mais atuais de segurança física e lógica,
- Os recursos humanos que gerem a plataforma têm formação e treino adequado para o serviço em questão.

4.2.2 PUBLICAÇÃO DE INFORMAÇÃO DE CERTIFICAÇÃO

A SISP mantém um repositório em ambiente Web, permitindo que as Partes Confiantes efectuem pesquisas on-line relativas à revogação e outra informação referente ao estado dos Certificados, durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

A SISP disponibiliza sempre a seguinte informação pública on-line no URL http://pki.sisp.cv:

- Seu proprio certificado
- Uma cópia electrónica actualizada desta DPC;
- Uma cópia electrónica actualizada da PC;
- Uma relação das Entidades Certificadoras vinculadas à SISP Root CA;
- Lista de Certificados Revogados das Entidades Certificadoras (LCR);
- Uma relação das Entidades de Registos vinculadas e seus respectivos endereços de instalações tecnicas em funcionamento;
- Formulario para solicitação de emissão de certificado;
- Formulario para solicitação de revogação de certificado.

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

4.2.3 FREQUENCIA DA PUBLICAÇÃO

A SISP garante que as actualizações a esta DPC e respectivas políticas serão publicadas sempre que houver necessidade de se proceder a uma alteração.

Uma nova LCR da SISP Root CA, será publicada sempre que se registar uma revogação. Se nenhuma revogação tiver sido produzida, a SISP Root CA disponibiliza uma nova LCR a cada 90 (noventa) dias.

Certificados das EC's subordinadas e certificados emitidos por estas, de acordo com a política definida na

respectiva DPC.

4.2.4 CONTROLO DE ACESSO

A informação publicada pela SISP estará disponível na Internet, sendo sujeita a mecanismos de controlo de acesso (acesso somente para leitura). A SISP implementou medidas de segurança lógica e física para impedir que pessoas não autorizadas possam adicionar, apagar ou modificar registos do repositório.

4.3 AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

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

Para além de auditorias de conformidade, a SISP irá efetuar outras fiscalizações e investigações para assegurar a conformidade da Entidades de Certificação constituintes da PKI da SISP com a legislação nacional bem como com os normativos internacionais aplicáveis. A execução destas auditorias internas, fiscalizações e investigações poderá ser delegada a uma entidade externa de auditoria.

No caso de Entidades de Certificação pertencentes à PKI da SISP mas operadas por outras entidades, a SISP pode, sempre que o entender, realizar auditorias internas às mesmas. Estas entidades são ainda obrigadas a, anualmente, entregar à SISP o relatório de auditoria anual, ou uma declaração de conformidade, realizado por uma entidade independente e reconhecida para o efeito.

4.3.1 AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

A SISP Root CA cumpre os requisitos definidos pela ICP-CV.

A auditoria é realizada por auditores qualificados pela ARME.

4.3.2 FREQUÊNCIA OU MOTIVO DA AUDITORIA

As práticas de certificação da SISP são alvo de auditorias periódicas, que terão como mínimo a periodicidade estipulada na lei, ou seja, uma periodicidade anual com a emissão de um relatório à data de 31 de Março do ano civil em causa. Esta auditoria será realizada por um Auditor credencido pela ARME.Esta auditoria é realizada tomando como base as normas existentes para o efeito sendo os seus resultados comunicados à entidade credenciadora que poderá tornar público o resultado de todo o processo.

No sentido de cumprir com estas obrigações, a SISP mantém registo de todas as operações do ciclo de vida dos certificados e de todas as comunicações mantidas com as entidades de registo/certificação por si reconhecida. Da mesma forma, a SISP obriga estas entidades a manter registo dos pedidos de subscrição recebidos e processado nos quais tenha estado envolvida.

Este registo deverá ser mantido num repositório de dados criado para o efeito e deverá poder ser confirmada através da análise dos registos das comunicações (em suporte eletrónico ou outro) com a entidade de certificação.

Para verificar o cumprimento destas disposições, a SISP conduzirá auditorias periódicas sobre as entidades de registo/certificação como forma de determinar a adequação dos procedimentos operacionais e níveis de

segurança tecnológicos às Políticas de Certificados suportadas. O não cumprimento das condições contratuais pode conduzir à suspensão e/ou revogação do(s) certificado(s) emitido(s)

5 . IDENTIFICAÇÃO E AUTENTICAÇÃO

5.1 ATRIBUIÇÃO DE NOMES

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

5.1.1 TIPOS DE NOMES

A atribuição de nomes segue a convenção determinada pela ICP-CV. A SISP garante a emissão de certificados contendo um Distinguished Name (DN) X.509, definido conforme RFC5280 e emite certificados para os requerentes que submetem documentação contendo um nome verificável.

A SISP assegurará, dentro da sua infraestrutura de confiança, a não existência de certificados que, contendo o mesmo DN, possam identificar entidades distintas.

5.1.2 NECESSIDADE DE NOMES SIGNIFICATIVOS

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

5.1.3 INTERPRETAÇÃO DE FORMATOS DE NOME

As regras utilizadas pela SISP para interpretar o formato dos nomes seguem o estabelecido no RFC 5280, assegurando que todos os atributos *DirectoryString* dos campos *issuer* e *subject* do certificado são codificados

numa *UTF8String,* com excepção dos atributos *country* e *serial number* que são codificados numa *PrintableString.*

5.1.4 UNICIDADE DOS NOMES

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

5.1.5 RESOLUÇÃO DE DISPUTAS DE NOMES

A SISP será responsável por atribuir e aprovar os DN`s. Será também responsável por resolver quaisquer disputas que possam surgir.

5.1.6 RECONHECIMENTO, AUTENTICAÇÃO E PAPÉIS DAS MARCAS REGISTADAS

Os nomes, emitidos pela SISP respeitarão o máximo possível as marcas registadas. A SISP não permitirá deliberadamente a utilização de nomes registados cuja propriedade não possa ser comprovada pelo requerente. Contudo poderá recusar a emissão de certificados com nomes de marcas registadas se entender que outra identificação é mais conveniente.

5.1.7 COMPROVAÇÃO DE POSSE DA CHAVE PRIVADA

Nos casos em que a SISP não seja a responsável pela geração do par de chaves criptográficas, a atribuir ao utilizador, a mesma assegurará que o utilizador possui a chave privada correspondente à chave pública constante no pedido de certificado antes de proceder à sua emissão.

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

5.2 VALIDAÇÃO DE IDENTIDADE NO REGISTO INICIAL

A SISP é responsável por autenticar a identidade das entidades candidatas à obtenção de um certificado.

Responsabiliza pela guarda de toda a documentação utilizada para verificação da identidade da entidade de certificação, garantindo a verificação da identidade dos seus representantes legais, por meio legalmente reconhecido e garantindo, no caso dos seus representantes legais não se encontrarem na cerimónia de emissão de certificado, os poderes bastantes do representante nomeado pela entidade para a referida emissão.

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

O documento que serve de base à emissão do certificado de uma EC contém, entre outros os seguintes elementos:

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

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

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

d) Endereço e outras formas de contacto;

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

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

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

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

5.2.1 ACORDO COM O SUBSCRITOR

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

1. Acordo dos termos e condições com o subscritor. Caso o subscritor do certificado seja distinto do sujeito, este último também será informado sobre os termos e condições;
2. Consentimento para a manutenção de registos por parte da SISP, com a informação usada no registo, bem como informação de subsequentes acontecimentos relativos ao acordo e ao seu objeto;
3. Permissão para passar esta informação a terceiros sob certas condições;
4. Permissão para passar informação sobre o estado dos certificados emitidos, ao abrigo do acordo, a terceiros não discriminados.

5.2.2 PEDIDO DE CERTIFICADO

A SISP:

1. Exigirá que uma entidade requerente de um certificado prepare e submeta os dados apropriados ao pedido, como especificado nesta DPC;
2. Quando necessário, exigirá que a entidade final requisitante submeta a sua chave pública para certificação, numa mensagem assinada digitalmente usando a chave privada a que corresponde a chave pública constante no pedido, de forma a:
    i. Permitir a deteção de erros no processo de certificação;
    ii. Provar a posse da chave privada relativa à chave pública a certificar.
3. Utiliza a chave pública contida no CSR, adiante designado de Pedido lógico de Certificado da entidade requisitante, para verificar a assinatura da entidade requisitante no Pedido lógico de Certificado submetido;
4. Verifica a autenticidade da submissão, da ER, de acordo com esta DPC;
5. Verificará a assinatura da ER no Pedido lógico de Certificado;
6. Verifica o Pedido lógico de Certificado para verificar se este contém erros ou omissões de acordo com esta DPC;
7. Verifica a unicidade do DN da entidade requisitante dentro da sua infraestrutura;
8. Aceita o Pedido lógico de Certificado vindo da entidade requisitante, cuja identidade foi validade;
9. Quando detetar chaves públicas repetidas o Pedido lógico de Certificado é rejeitado.

5.3 AUTENTICAÇÃO PRESENCIAL DE ENTIDADES INDIVIDUAIS

A autenticação presencial do representante autorizado das organizações candidatas a um certificado será baseada em, pelo menos, duas formas de identificação emitidas pelo governo (em que pelo menos uma terá de ser um documento com fotografia, tal como, um passaporte ou bilhete de identidade). A capacidade da

pessoa agir em nome da organização candidata será também autenticada, através da apresentação de documentação em papel, indicando este facto.

A informação descrita acima tem de ser validada pela SISP aquando da devolução dos formulários de inscrição completamente preenchidos. A SISP ou Entidade de Registo por ela designada, será responsável por verificar a identidade dos representantes pessoalmente.

5.4 IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDOS DE RENOVAÇÃO DE CHAVES

5.4.1 IDENTIFICAÇÃO E AUTENTICAÇÃO PARA RENOVAÇÃO DE CHAVES, DE ROTINA

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

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

- indivíduo/organização ainda existe e autorizou a emissão do certificado;
- indivíduo/organização continua a obedecer aos requisitos de associação;
- indivíduo/organização possui a chave privada correspondente à nova chave pública expedida para certificação;
- A SISP aceita a continuidade do indivíduo/organização dentro da sua hierarquia.

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

5.4.2 RENOVAÇÃO APÓS REVOGAÇÃO

Se um certificado é revogado, o indivíduo/organização será sujeito a todo o processo inicial de registo, de forma a obter um novo certificado.

5.5 PEDIDO DE REVOGAÇÃO

O pedido de revogação deve obedecer às condições descritas em pormenor na secção 6.7.

6. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

6.1 PEDIDO DE CERTIFICADOS

O pedido de certificado deve ser formulado, mediante o preenchimento do Formulario proprio, disponivel no respositório da PKI da SISP em http://pki.sisp.cv.

6.2 EMISSÃO DOS CERTIFICADOS

6.2.1 PROCEDIMENTO PARA A EMISSÃO DE CERTIFICADO

A emissão do certificado é efetuada por meio de uma cerimónia que decorre na zona de alta segurança da PKI da SISP e, em que se encontram presentes:

- Os representantes legais da entidade subordinada requerente ou o(s) representante(s) nomeado(s) para esta cerimónia;
- Pelo menos 3 membros dos Grupos de Trabalho;
- Um Auditor da ARME na geração do par de chaves da SISP Root CA e o Auditor SISP no caso das Sub CA's;
- Quaisquer observadores, aceites simultaneamente pelos membros do Grupo de Trabalho e pelos representantes da entidade subordinada requerente.

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

- Identificação e autenticação de todas as pessoas presentes na cerimónia, garantindo que o(s) representante(s) e os membros do Grupo de Trabalho têm os poderes necessários para os atos a praticar;
- Os membros do Grupo de Trabalho efetuam o procedimento de arranque de processamento do certificado e emitem o Pedido de Assinatura de Certificado (CSR) (correspondente ao PKCS#10 gerado no HSM), que é arquivado num suporte tecnológico (não regravável);
- O certificado emitido e assinado pela Entidade Certificadora hierarquicamente superior, é importado na EC correspondente;
- Procede-se á geração da primeira CRL;
  A cerimónia de emissão fica concluida com a execução do procedimento de finalização de processamento do certificado, pelos membros do Grupo de Trabalho;

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

6.2.2 NOTIFICAÇÃO DA EMISSÃO DO CERTIFICADO AO TITULAR

A emissão do certificado é efetuada de forma presencial, de acordo com a secção anterior.

6.3 ACEITAÇÃO DO CERTIFICADO

6.3.1 PROCEDIMENTO PARA A ACEITAÇÃO DE CERTIFICADO

O certificado considera-se aceite após a assinatura do formulário de emissão e aceitação de certificado pelo(s) representante(s) da entidade subordinada, de acordo com a cerimónia de emissão (conforme secção 6.2.1).

Note-se que antes de ser disponibilizado o certificado aos representantes, e consequentemente lhe serem disponibilizadas todas as funcionalidades na utilização da chave privada e certificado, é garantido que:

- É tomado conhecimento dos direitos e responsabilidades;
- É tomado conhecimento das funcionalidades e conteúdo do certificado;
- É aceite formalmente o certificado e as suas condições de utilização assinando para o efeito o Formulário de Receção de certificado.

6.3.2 PUBLICAÇÃO DO CERTIFICADO

A SISP Root CA não publica os certificados emitidos, disponibilizando-o integralmente aos representantes, nas condições definidas no ponto 6.3.1.

6.3.3 NOTIFICAÇÃO DA EMISSÃO DE CERTIFICADO A OUTRAS ENTIDADES

Nada a assinalar.

6.3.4 USO DO CERTIFICADO E DA CHAVE PRIVADA PELO TITULAR

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

A sua utilização apenas é permitida:

- A quem estiver designado no campo "Subject" do certificado;
- De acordo com as condições definidas na secção 3.5;
- Enquanto o certificado se mantiver válido e não estiver na CRL da SISP Root CA.

Adicionalmente:

- O certificado da EC subordinada pode ser utilizado para assinar certificados e respetiva CRL, assim como certificados necessários para a operação e serviços da EC subordinados;
- O certificado de Validação on-line OCSP tem como objetivo a sua utilização em servidores OCSP.

6.3.5 USO DO CERTIFICADO E DA CHAVE PÚBLICA PELAS PARTES CONFIANTES

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

- Ter conhecimento e perceber a utilização e funcionalidades proporcionadas pela criptografia de chave pública e certificados;
- Ser responsável pela sua correta utilização;
- Ler e entender os termos e condições descritos nas políticas e práticas de certificação;
- Verificar os certificados (validação de cadeias de confiança) e CRL, tendo especial atenção às suas extensões marcadas como críticas e propósito das chaves;
- Confiar nos certificados, utilizando-os sempre que estes estejam válidos.

6.4 RENOVAÇÃO DE CERTIFICADOS

Esta prática não é suportada pela PKI da SISP.

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

6.4.1 MOTIVOS PARA RENOVAÇÃO DE CERTIFICADO
Nada a assinalar.

6.4.2 QUEM PODE SUBMETER O PEDIDO DE RENOVAÇÃO DE CERTIFICADO
Nada a assinalar.

6.4.3 PROCESSAMENTO DO PEDIDO DE RENOVAÇÃO DE CERTIFICADO
Nada a assinalar.

6.4.4 NOTIFICAÇÃO DE EMISSÃO DE NOVO CERTIFICADO AO TITULAR
Nada a assinalar.

6.4.5 PROCEDIMENTOS PARA ACEITAÇÃO DE CERTIFICADO
Nada a assinalar.

6.4.6 PUBLICAÇÃO DE CERTIFICADO APÓS RENOVAÇÃO
Nada a assinalar.

6.4.7 NOTIFICAÇÃO DA EMISSÃO DO CERTIFICADO A OUTRAS ENTIDADES
Nada a assinalar.

6.5 RENOVAÇÃO DE CERTIFICADO COM GERAÇÃO DE NOVO PAR DE CHAVES

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

A renovação de certificado com geração de novo par de chaves é feita de acordo com o estabelecido na secção 6.2.

6.5.1 MOTIVO PARA A RENOVAÇÃO DE CERTIFICADO COM GERAÇÃO DE NOVO PAR DE CHAVES

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

- certificado está a expirar;
- par de chaves está a atingir o período de utilização previsto;
- A informação que deu origem ao certificado sofre alterações.

6.5.2 QUEM PODE SUBMETER O PEDIDO DE CERTIFICAÇÃO DE UMA NOVA CHAVE PÚBLICA
Tal como na secção 6.1.

6.5.3 PROCESSAMENTO DO PEDIDO DE RENOVAÇÃO DE CERTIFICADO COM GERAÇÃO DE NOVO PAR DE CHAVES
Tal como na secção 6.2.

6.5.4 NOTIFICAÇÃO DA EMISSÃO DE NOVO CERTIFICADO AO TITULAR
Tal como na secção 6.2.2.

6.5.5 PROCEDIMENTOS PARA ACEITAÇÃO DE UM CERTIFICADO RENOVADO COM GERAÇÃO DE NOVO PAR DE CHAVES

Tal como na secção 6.3.1.

6.5.6 PUBLICAÇÃO DE CERTIFICADO RENOVADO COM GERAÇÃO DE NOVO PAR DE CHAVES

Tal como na secção 6.3.2.

6.5.7 NOTIFICAÇÃO DA EMISSÃO DE CERTIFICADO RENOVADO A OUTRAS ENTIDADES

Tal como na secção 6.3.3.

6.6 MODIFICAÇÃO DE CERTIFICADOS

Esta prática não é suportada pela PKI da SISP.

A alteração de certificados é o processo em que é emitido um certificado para um titular, mantendo as respetivas chaves, havendo apenas alterações na informação do certificado.

6.6.1 MOTIVOS PARA ALTERAÇÃO DO CERTIFICADO

Nada a assinalar.

6.6.2 QUEM PODE SUBMETER O PEDIDO DE ALTERAÇÃO DE CERTIFICADO

Nada a assinalar.

6.6.3 PROCESSAMENTO DO PEDIDO DE ALTERAÇÃO DE CERTIFICADO

Nada a assinalar.

6.6.4 NOTIFICAÇÃO DA EMISSÃO DE CERTIFICADO ALTERADO AO TITULAR

Nada a assinalar.

6.6.5 PROCEDIMENTOS PARA ACEITAÇÃO DE CERTIFICADO ALTERADO

Nada a assinalar.

6.6.6 PUBLICAÇÃO DO CERTIFICADO ALTERADO

Nada a assinalar.

6.6.7 NOTIFICAÇÃO DA EMISSÃO DE CERTIFICADO ALTERADO A OUTRAS ENTIDADES

Nada a assinalar.

6.7 SUSPENSÃO E REVOGAÇÃO DE CERTIFICADOS

6.7.1 CIRCUNSTÂNCIAS PARA SUSPENSÃO

A SISP Root CA não efetua suspensões.

6.7.2 QUEM PODE PEDIR A SUSPENSÃO

Nada a assinalar.

6.7.3 PROCEDIMENTO PARA UM PEDIDO DE SUSPENSÃO

Nada a assinalar.

6.7.4 LIMITES DO PERÍODO DE SUSPENSÃO

Nada a assinalar.

6.7.5 MOTIVOS PARA REVOGAÇÃO

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

Os certificados depois de revogados, deixam de ser válidos.

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

- Comprometimento da chave privada (SISP Root CA ou EC subordinada);
- Perda da chave privada;
- Incorreções graves nos dados fornecidos;
- Perda, destruição ou deterioração do dispositivo de suporte da chave privada (por exemplo, suporte/token criptográfico);
- Comprometimento da senha de acesso à chave privada
  (exemplo: PIN);
- Utilização do certificado para atividades abusivas;
- Risco de comprometimento da chave (por exemplo, devido à fraqueza do algoritmo ou tamanho de chave);
- Por ordem judicial ou, desde que devidamente fundamentada, pelas entidades integrantes da ICP-CV a saber:
  - Conselho Gestor da ICP-CV
  - Autoridade Credenciadora
  - ECR-CV
- Cessação de funções.

O certificado é revogado no prazo máximo de 24 horas.

6.7.6 SOLICITAR A REVOGAÇÃO

Está legitimado para submeter o pedido de revogação, sempre que se verifiquem alguma das condições descritas no ponto 6.7.5, os seguintes entidades:

- Os responsáveis legais da Entidade de Certificação Subordinada;
- A SISP S.A.;
- Uma parte confiante, sempre que demonstre que o certificado foi utilizado com fins diferente dos previstos.

A SISP Root CA guarda toda a documentação utilizada para verificação da identidade e autenticidade da entidade que efetua o pedido de revogação, garantindo a verificação da identidade dos seus representantes legais, por meio legalmente reconhecido, não aceitando poderes de representação para o pedido de revogação do certificado da SISP Root CA e nem das Entidades Certificadoras Subordinadas.

6.7.7 PROCEDIMENTO PARA SOLICITAÇÃO DE REVOGAÇÃO

Todos os pedidos de revogação devem ser endereçados à SISP S.A. por escrito ou por mensagem eletrónica assinada digitalmente, em formulário próprio de pedido de revogação, observando o seguinte:

- Identificação e autenticação da entidade que efetua o pedido de revogação;
- Registo e arquivo do formulário de pedido de revogação;
- Análise do pedido de revogação pelo Grupo de Trabalho de Autenticação da PKI da SISP, que propõe ao Grupo de Trabalho de Gestão a aprovação ou recusa do pedido de revogação;
- Mediante o parecer do Grupo de Trabalho de Autenticação da PKI da SISP, o Grupo de trabalho de Gestão, decide a aprovação ou recusa do pedido de revogação do certificado;
- Sempre que se decidir revogar um certificado, a revogação é publicada na respetiva CRL.

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

- Data do pedido de revogação;
- Nome do titular do certificado;
- Exposição pormenorizada dos motivos para o pedido de revogação;

- Nome e funções da pessoa que solicita a revogação;
- Informação de contacto da pessoa que solicita a revogação;
- Assinatura da pessoa que solicita a revogação.

6.7.8 PROCESSAMENTO DO PEDIDO DE REVOGAÇÃO

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

6.7.9 REQUISITOS DE VERIFICAÇÃO DA REVOGAÇÃO PELAS PARTES CONFIANTES

Antes de utilizarem um certificado, as partes confiantes têm como responsabilidade verificar o estado de todo os certificados, através das CRL ou num servidor de verificação do estado online (via OCSP).

6.7.10 FREQUÊNCIA DE EMISSÃO DE CRL`S (SE APLICÁVEL)

A SISP Root CA publica uma nova CRL no repositório, sempre que haja uma revogação. Quando não existam alterações ao estado de validade dos certificados, ou seja, se nenhuma revogação se tiver produzido, a SISP Root CA disponibiliza uma nova CRL a cada 3 meses.

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

Todas as CRL`s emitidas pela SISP são assinadas digitalmente pela SISP.

6.7.11 REQUISITOS PARA VERIFICAÇÃO DE CRL`S

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

6.7.12 OUTRAS FORMAS DE ANÚNCIO DE REVOGAÇÃO

Nada a assinalar.

7. MEDIDAS DE SEGURANÇA FISICA, DE GESTÃO E OPERACIONAIS

A SISP implementou várias regras e políticas incidindo sobre controlos físicos, procedimentais e humanos, que suportam os requisitos de segurança constantes nesta DPC.

Estas regras e policticas seguem as boas praticas recomendadas pelos principais standards interncaionais relativos á segurança de informação, designadamente ISO 27001.

7.1 MEDIDAS DE SEGURANÇA FÍSICA

7.1.1 LOCALIZAÇÃO FÍSICA E TIPO DE CONSTRUÇÃO

As instalações da PKI da SISP foram desenhadas de forma a proporcionar um ambiente capaz de controlar e auditar o acesso aos sistemas de certificação, estando fisicamente protegidas do acesso não autorizado, dano ou interferência. A arquitetura utiliza o conceito de defesa em profundidade, ou seja, por níveis de segurança, garantindo-se que o acesso a um nível de segurança mais elevado só é possível quando previamente se tenha alcançado o nível imediatamente anterior.

7.1.2 ACESSO FÍSICO AO LOCAL

Os sistemas da PKI da SISP estão protegidos por um mínimo de 4 níveis de segurança física hierárquicos, garantindo-se que o acesso a um nível de segurança mais elevado só é possível quando previamente se tenha alcançado os privilégios necessários ao nível imediatamente anterior.

Atividades operacionais sensíveis da EC, criação e armazenamento de material criptográfico, quaisquer atividades no âmbito do ciclo de vida do processo de certificação como autenticação, verificação e emissão ocorrem dentro da zona mais restrita de alta segurança. Acessos físicos são automaticamente registados e gravados para efeitos de auditorias.

7.1.3 ENERGIA E AR CONDICIONADO

O ambiente seguro do PKI da SISP possui equipamento redundante, que garante condições de funcionamento 24 horas por dia / 7 dias por semana, de:

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

- Refrigeração/ventilação/ar condicionado que controlam os níveis de temperatura e humidade, garantindo condições adequadas para o correto funcionamento de todos os equipamentos

eletrónicos e mecânicos presentes dentro do ambiente.

7.1.4 EXPOSIÇÃO À ÁGUA

Nada a assinalar.

7.1.5 PREVENÇÃO E PROTEÇÃO CONTRA INCÊNDIO

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

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

7.1.6 SALVAGUARDA DE SUPORTES DE ARMAZENAMENTO

Todos os suportes de informação sensível são guardados em cofres e armários de segurança dentro da zona de alta segurança, assim como num ambiente distinto externo ao edifício com controlos de acessos físicos e lógicos apropriados para restringir o acesso apenas a elementos autorizados dos Grupos de Trabalho

7.1.7 ELIMINAÇÃO DE RESÍDUOS

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

É garantido que não é possível recuperar nenhuma informação dos suportes de informação utilizados para armazenar ou transmitir informação sensível, antes dos mesmos serem eliminados. Equipamentos criptográficos ou chaves físicas de acesso lógico são fisicamente destruídos ou seguem as recomendações de destruição do respetivo fabricante, antes da sua eliminação.

Outros equipamentos de armazenamento (discos rígidos, tapes, ...) são devidamente limpos de modo a não ser possível recuperar nenhuma.

7.1.8 INSTALAÇÕES EXTERNAS (ALTERNATIVA) PARA RECUPERAÇÃO DE SEGURANÇA

As instalações alternativas têm os mesmos níveis de segurança do principal.

7.2 MEDIDA DE SEGURANÇA DOS PROCESSOS

A atividade de uma Entidade Certificadora (doravante denominada por EC) depende da intervenção coordenada e complementar de um extenso elenco de recursos humanos, nomeadamente porque:

- Dados os requisitos de segurança inerentes ao funcionamento de uma EC é vital garantir uma

adequada segregação de responsabilidades, que minimize a importância individual de cada um dos intervenientes;

- É necessário garantir que a EC apenas poderá ser sujeita a ataques do tipo denial-of-service mediante o conluio de um número significativo de intervenientes;
- Quando uma mesma entidade é detentora de várias EC de diferentes níveis de segurança ou hierarquia, por vezes é desejável que os recursos humanos associados a uma EC não acumulem funções (ou pelo menos as mesmas) numa EC distinta.

Pelo exposto, nesta seção, descrevem-se os requisitos necessários para reconhecer os papéis de confiança e responsabilidades associadas a cada um desses papéis. Esta secção inclui também a separação de deveres, em termos dos papéis que não podem ser executados pelos mesmos indivíduos.

7.2.1 GRUPOS DE TRABALHO

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

A PKI da SISP estabeleceu que os papéis de confiança fossem agrupados em seis categorias diferentes (que correspondem a cinco Grupos de Trabalho distintos) de modo a garantir que as operações sensíveis sejam efetuadas por diferentes pessoas autenticados, eventualmente pertencentes a diferentes Grupos de Trabalho, assegurando que existem dois membros em cada grupo

7.2.1.1 GRUPO DE TRABALHO DE AUDITORIA

É responsável por efetuar a auditoria interna a todas as ações relevantes e necessárias para assegurar a operacionalidade da EC..

As responsabilidades deste grupo são:

- Auditar a execução e confirmar a exatidão dos processos e cerimónias da EC;
- Registar todas as operações sensíveis;
- Investigar suspeitas de fraudes procedimentais;
- Verificar periodicamente a funcionalidade dos controlos de segurança (dispositivos de alarme, de controlo de acessos, sensores de fogo, etc.) existentes nos vários ambientes;
- Verificar periódicamente, a integridade dos Ambientes de Custódia, assegurando que lá se encontram os artefactos respectivos e que estão devidamente identificados;
- Registar todos os procedimentos passíveis de auditoria;
- Registar os resultados de todas as ações por si realizadas;
- Assumir o papel de “Auditor de Sistema”;
- Validar que todos os recursos utilizados são seguros.

7.2.1.2 GRUPO DE SEGURANÇA

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

Contsituem responsabilidades deste grupo:

- Gerir o Ambiente de Administração de Segurança;
- Definir e gerir todas as políticas da EC e garantir que se encontram actualizadas e adaptadas à sua realidade;
- Garantir implementação das políticas definidas;
- Assegurar que as PCs da EC são suportadas pela DPC da EC;
- Assegurar que todos os documentos relevantes e relacionados, directa ou indirectamente, com o funcionamento da EC e existentes em formato papel se encontram armazenados no Ambiente de Informação;
- Gerir e controlar os sistemas de segurança física, incluindo acessos, do ambiente de produção;

- Explicar todos os mecanismos de segurança aos funcionários que devam conhecê-los e de consciencializá-los para as questões de segurança levando-os a fazer cumprir as normas e políticas de seguranças estabelecidas;
- Calendarizar cerimónias para testes, formações e auditoria dos sistemas de informação;
- Configurar os acessos à aplicação da EC (grupos, regras, logs);
- Configurar perfis de certificados na aplicação da EC;
- Activar a interface de operação da EC;
- Activar as chaves para sua utilização;
- Autorizar a geração de chaves da aplicação. Esta operação é requerida durante a cerimónia de geração de chaves para a EC;
- Arranque do interface de configuração da SISP ROOT CA.

Adicionalmente na função de administração/operação de HSM

- Recuperação da funcionalidade do hardware criptográfico em caso de falha de um HSM;
- Recuperação de chaves em caso de terem sido apagadas acidentalmente;
- Substituição de um conjunto de cartões de administrador. Esta operação só é necessária ser realizada se se deseja ampliar ou reduzir o número de cartões de administrador;
- Substituição de um conjunto de cartões de operador. Esta operação só é necessaria se deseja ampliar ou reduzir o número de cartões de operador ou substituir algum cartão deteriorado;
- Ampliação do número de HSM integrados na infraestrutura;
- Dado que se opera em modo FIPS140-2 Nível 3, autorização para a geração de conjuntos de cartões de operador e chaves. Esta operação só se requere durante a cerimónia de geração de chaves da EC.
- Ativação de chaves para sua utilização. Isto significa que cada vez que se inicie a EC, é necessário a inserção dos cartões de operadores associados às chaves;
- Autorização para a geração de chaves da aplicação. Esta operação só é requerida durante a cerimónia de geração de chaves para a EC;
- Arranque do interface de configuração da EC e do resto das entidades que formam a PKI.

7.2.1.3 GRUPO DE ADMINISTRAÇÃO DE SISTEMAS

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

As responsabilidades deste grupo são:

- Manter um inventário actualizado de todos os produtos relacionados com a EC;
- Instalar, interligar e configurar o *hardware* da EC;
- Instalar e configurar o *software* de base da EC;
- Gerir e actualizar os produtos instalados;
- Preparar comunicados sobre as palavras-chave iniciais;
- Preparar comunicados sobre as Hash do(s) CD(s) de instalação utilizados.

Adicionalmente, compete ao Grupo

- Operar diariamente os sistemas, realizando cópias de segurança e reposição de informação, caso necessário;
- Realizar as tarefas de rotina da EC, incluindo operações de cópias de segurança dos seus sistemas;
- Gerir o Ambiente de Operação.

7.2.1.4 GRUPO DE REGISTOS

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

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

7.2.1.4 GRUPO DE GESTÃO

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

As responsabilidades deste grupo são:

- Rever e aprovar as políticas propostas pelo Grupo de Trabalho de Administração de Segurança;
- Pedir a aprovação de Políticas ao CG da ICP-CV;
- Designar os membros dos restantes grupos de trabalho;
- Disponibilizar a identificação de todos os indivíduos que pertencem aos vários Grupos de Trabalho, em um ou mais pontos de acesso facilmente acessíveis pelos indivíduos autorizados.

7.2.2 NÚMERO DE PESSOAS EXIGIDAS POR TAREFA

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

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

7.2.3 FUNÇÕES QUE REQUEREM SEPARAÇÃO DE RESPONSABILIDADES

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

Grupo de Trabalho	Incompativel com				
	(a)	(b)	(c)	(d)	(e)
Administração de Segurança (a)		X	X	X	
Administração de Sistemas (b)	X		X	X	
Administração de Registo (c)	X	X		X	
Auditoria (d)	X	X	X		X
Gestão (e)				X	

7.3 MEDIDAS DE SEGURANÇA DE PESSOAL

7.3.1 REQUISITOS RELATIVOS ÀS QUALIFICAÇÕES, EXPERIÊNCIA, ANTECEDENTES E CREDENCIAÇÃO

Todo o pessoal que desempenhe funções de confiança na PKI da SISP deve cumprir os seguintes requisitos:

- Ter sido nomeado formalmente para a função a desempenhar;
- Apresentar provas de antecedentes, qualificações e experiência necessárias para a realização das tarefas inerentes à sua função;
- Ter recebido formação e treino adequado para o desempenho da respetiva função;
- Garantir confidencialidade, relativamente a informação sensível sobre a EC ou dados de identificação dos titulares;
- Garantir o conhecimento dos termos e condições para o desempenho da respetiva função e,
- Garantir que não desempenha funções que possam causar conflito com as suas responsabilidades nas atividades da EC.

7.3.2 PROCEDIMENTO DE VERIFICAÇÃO DE ANTECEDENTES

A verificação de antecedentes decorre do processo de credenciação dos indivíduos nomeados para exercer cargos em qualquer uma das funções de confiança. A verificação de antecedentes inclui:

- Confirmação de identificação, usando documentação emitida por fontes fiáveis e,
- Investigação de registos criminais.

7.3.3 REQUISITOS DE FORMAÇÃO E TREINO

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

Os elementos dos Grupos de Trabalho, estão adicionalmente sujeitos a um plano de formação e treino, englobando os seguintes tópicos:

- Certificação digital e Infraestruturas de Chave Pública;
- Conceitos gerais sobre segurança da informação;

- Formação específica para o seu papel dentro do Grupo de Trabalho;
- Funcionamento do software e/ou hardware usado na PKI da SISP;
- Política de Certificados e Declaração de Práticas de Certificação;
- Recuperação face a desastres;
- Procedimentos para a continuidade da atividade e,

- Aspetos legais básicos relativos à prestação de serviços de certificação.

7.3.4 FREQUÊNCIA E REQUISITOS PARA AÇÕES DE RECICLAGEM

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

- Sempre que exista qualquer alteração tecnológica, introdução de novas ferramentas ou modificação de procedimentos, é levada a cabo a adequada formação para todo o pessoal afeto à PKI da SISP;
- Sempre que são introduzidas alterações nas Políticas de Certificação ou Declaração de Práticas de Certificação são realizadas sessões de reciclagem aos elementos da PKI da SISP.

7.3.5 FREQUÊNCIA E SEQUÊNCIA DA ROTAÇÃO DE FUNÇÕES

Nada a assinalar.

7.3.6 SANÇÕES PARA AÇÕES NÃO AUTORIZADAS

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

São aplicadas sanções de acordo com as regras da PKI da SISP e das leis de segurança nacional, a todos os indivíduos que realizem ações não autorizadas ou que façam uso não autorizado dos sistemas.

7.3.7 REQUISITOS PARA PRESTADORES DE SERVIÇOS

Consultores ou prestadores de serviços independentes, tem permissão de acesso à zona de alta segurança desde de que estejam sempre acompanhados e diretamente supervisionados pelos membros do Grupo de Trabalho e ficando o seu acesso registado no Livro de Presenças próprio.

7.3.8 DOCUMENTAÇÃO FORNECIDA AO PESSOAL

É disponibilizado aos membros dos Grupos de Trabalho toda a informação adequada para que estes possam realizar as suas tarefas de modo competente e satisfatório.

7.4 PROCEDIMENTOS DE AUDITORIA DE SEGURANÇA

7.4.1 TIPO DE EVENTOS REGISTADOS

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

- Tentativas de acesso (com e sem sucesso) para solicitar, gerar, assinar, emitir ou revogar chaves de certificados;
- Tentativas de acesso (com e sem sucesso) para criar, modificar ou apagar informação dos titulares dos certificados;
- Tentativas de acesso (com e sem sucesso) e alterações dos parâmetros de segurança do sistema operativo;
- Emissão e publicação de CRL's;
- Arranque e paragem de aplicações;
- Tentativas de acesso (com e sem sucesso) de início e fim de sessão;
- Tentativas de acesso (com e sem sucesso) de criar, modificar, apagar contas do sistema;
- Cópias de segurança, recuperação ou arquivo dos dados;
- Alterações ou atualizações de software e hardware;
- Manutenção dos sistemas;
- Operações realizadas por membros dos Grupos de Trabalho;
- Alteração de Recursos Humanos;
- Tentativas de acesso (com e sem sucesso) às instalações por parte de pessoal autorizado ou não;
- A cerimónia de geração de chaves e sistemas envolvidos na mesma, tais como servidores aplicacionais, base de dados e sistema operativo.

7.4.2 FREQUÊNCIA DA AUDITORIA DE REGISTOS

Os registos são analisados e revistos na base diária e de forma automatizada, produzindo o envio de alertas para o grupo de trabalho de Auditoria, sempre que haja suspeitas ou atividades anormais ou ameaças de algum tipo. Ações tomadas, baseadas na informação dos registos são também documentadas.

7.4.3 PERÍODO DE RETENÇÃO DOS REGISTOS DE AUDITORIA

Os registos estão disponíveis online durante o período de validade da certificação, findo o qual são arquivados nos termos descritos na secção 8.5.

7.4.4 PROTEÇÃO DOS REGISTOS DE AUDITORIA

Os registos são analisados exclusivamente por membros do Grupo de Trabalho de Auditoria e reportados ao Grupo de Gestão.

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

As cópias de segurança dos registos da PKI da SISP são armazenadas em local seguro e em cofres que cumprem a norma EN 1143.

A destruição de um arquivo de auditoria em offline só poderá ser efetuada após autorização expressa do Grupo de Gestão e executada na presença de, no mínimo dois elementos, um elemento de segurança e um de auditoria, sendo que este ato deverá ficar registado em log de Auditoria.

7.4.5 PROCEDIMENTOS PARA A CÓPIA DE SEGURANÇA DOS REGISTOS

São criadas cópias de segurança regulares dos registos em sistemas de armazenamento de alta capacidade, nomeadamente em tape e em storage.

7.4.6 SISTEMA DE RECOLHA DE REGISTOS (INTERNO / EXTERNO)

O processo de tratamento e recolha de registos de auditoria é constituído por uma combinação de processos automáticos e manuais, executados pelos sistemas operativos, pelas aplicações da PKI da SISP e pelo pessoal que as opera. Todos os registos de auditoria são armazenados nos sistemas internos da PKI da SISP.

7.4.7 NOTIFICAÇÃO DE AGENTES CAUSADORES DE EVENTOS

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

7.4.8 AVALIAÇÃO DE VULNERABILIDADES

Os registos auditáveis, são regularmente analisados de modo a minimizar e eliminar potenciais tentativas de quebrar a segurança do sistema. São realizados quatro testes de intrusão por ano, de forma a verificar e avaliar vulnerabilidades. O resultado da análise é reportado ao Grupo de Gestão da PKI da SISP para rever e aprovar um plano de implementação e correção das vulnerabilidades detetadas.

7.5 ARQUIVO DE REGISTOS

7.5.1 TIPO DE DADOS ARQUIVADOS

Todos os dados auditáveis, são arquivados (conforme indicado na secção 8.4.1), assim como informação de pedidos de certificados e documentação de suporte ao ciclo de vida das várias operações.

As informações e eventos que são registados e arquivados são:

- Os registos de auditoria especificados no ponto 8.4.1 desta DPC;
- As cópias de segurança dos sistemas que compõem a infraestrutura da PKI da SISP;
- Toda a documentação relativa ao ciclo de vida dos certificados, designadamente:
    - Procedimentos de emissão e revogação de certificados de serviço;
    - Formulários de emissão e receção dos certificados de serviço;
- Acordos de confidencialidade;

- Protocolos estabelecidos com as Entidades Subscritoras;
- Contratos estabelecidos entre a PKI da SISP e outras entidades - apenas disponibilizados a quem solicitar a sua visualização, após avaliação e aprovação prévia do pedido;
- Autorizações de acesso aos sistemas de informação;
- Acessos aos artefactos existentes nas custódias.

7.5.2 PERÍODO DE RETENÇÃO EM ARQUIVO

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

7.5.3 PROTEÇÃO DOS ARQUIVOS

O arquivo é protegido de modo a que:

- Apenas membros autorizados dos Grupos de Trabalho possam consultar e ter acesso ao arquivo;
- arquivo é protegido contra qualquer modificação ou tentativa de o remover;
- arquivo é protegido contra a deterioração dos media onde é guardado, através de migração periódica para media novo;
- arquivo é protegido contra a obsolescência do hardware, sistemas operativos e outros software, pela conservação do hardware, sistemas operativos e outros software que passam a fazer parte do próprio arquivo, de modo a permitir o acesso e uso dos registos guardados, de modo intemporal;
- Os arquivos são guardados de modo seguro em ambientes externos seguros, de acordo com a Politica de Retenção de Dados. As cópias de segurança da PKI da SISP são armazenadas em locais seguros e em cofres que cumprem a norma EN 1143.

7.5.4 PROCEDIMENTOS PARA AS CÓPIAS DE SEGURANÇA DO ARQUIVO

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

7.5.5 REQUISITOS PARA VALIDAÇÃO CRONOLÓGICA DOS REGISTOS

Algumas das entradas dos arquivos contêm informação de data e hora, que é prestado por um serviço preciso de referência temporal. T

7.5.6 SISTEMA DE RECOLHA DE DADOS DE ARQUIVO (INTERNO / EXTERNO)

Os sistemas de recolha de dados de arquivo são internos.

7.5.7 PROCEDIMENTOS DE RECUPERAÇÃO E VERIFICAÇÃO DE INFORMAÇÃO ARQUIVADA

Apenas membros autorizados dos Grupos de Trabalho têm acesso aos arquivos para verificação da sua integridade.

São realizadas de forma automática verificações de integridade dos arquivos eletrónicos (cópias de segurança) na altura da sua criação, em caso de erros ou comportamentos imprevistos, deve-se realizar novo arquivo.

7.6 RENOVAÇÃO DE CHAVES

Apenas as entidades de certificação subordinadas da PKI da SISP com certificados válidos podem requerer a renovação do respetivo par de chaves, desde que a geração de novo par de chaves esteja conforme a secção 7.7.

7.7 RECUPERAÇÃO EM CASO DE DESASTRE OU COMPROMETIMENTO

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

7.7.1 PROCEDIMENTOS EM CASO DE INCIDENTE OU COMPROMETIMENTO

As cópias de segurança das chaves privadas da SISP Root CA (geradas e mantidas de acordo com a secção 8.2.3.1) e dos registos arquivados (secção 7.5.1) são guardados em ambientes seguros externos e disponíveis em caso de desastre. No caso de comprometimento da chave privada da SISP Root CA, esta deverá tomar as seguintes ações:

- Proceder à sua revogação imediata;
- Revogar todos os certificados dela, dependentes;
- Informar todos os titulares dos seus certificados e terceiras partes conhecidas;
- Informar todas as Entidades que compõem a PKI da SISP.

7.7.2 CORRUPÇÃO DOS RECURSOS INFORMÁTICOS, DO SOFTWARE E/OU DOS DADOS

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

Se for confirmado que os recursos informáticos, software e/ou dados estão corrompidos, devem ser tomadas medidas apropriadas de resposta ao incidente. A resposta ao incidente pode incluir o restabelecimento do equipamento/dados corrompidos, utilizando equipamento similar e/ou recuperando cópias de segurança e registos arquivados. Até que sejam repostas as condições seguras, a SISPCA01Root suspenderá os seus serviços e notificará todas as Entidades envolvidas. Caso se verifique que esta situação tenha afetado certificados emitidos, proceder-se-á à notificação dos titulares dos mesmos e à revogação dos respetivos certificados.

7.7.3 PROCEDIMENTOS EM CASO DE COMPROMETIMENTO DA CHAVE PRIVADA DA ENTIDADE

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

- Informar a Autoridade Credenciadora Nacional e o Conselho Gestor da ICP-CV;
- Notificação das EC subordinadas, todos os titulares de certificados emitidos no “ramo” da hierarquia de confiança da SISP Root CA;

- Revogação do certificado da SISP Root CA e de todos os certificados emitidos no “ramo” da hierarquia

de confiança da SISP Root CA;

- Geração de novo par de chaves para a SISP Root CA e inclusão nos vários sistemas/browsers;
- Renovação de todos os certificados emitidos no "ramo" da hierarquia de confiança da SISP Root CA.

7.7.4 CAPACIDADE DE CONTINUIDADE DA ATIVIDADE EM CASO DE DESASTRE

A PKI da SISP dispõe dos recursos de computação, software, cópias de segurança e registos arquivados nas suas instalações secundárias de segurança, necessários para restabelecer ou recuperar operações essenciais (emissão e revogação de certificados, com a publicação de informação de revogação) com base em procedimentos definidos no Plano de Contingência, após um desastre natural ou outro.

7.8 PROCEDIMENTOS EM CASO DE EXTINÇÃO DA EC OU ER

Em caso de cessação de atividade como prestador de serviços de Certificação, a SISP executa os procedimentos previstos no Plano de Cessação de Actividades, conforme artigo 36º do DL nº33/2007.:

Em caso de alterações do organismo/estrutura responsável de gestão da atividade da EC, esta deve informar de tal facto à Autoridade Credenciadora Nacional e ao Conselho Gestor da IPC-CV.

8. MEDIDAS DE SEGURANÇA TECNICAS

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

8.1 GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES

A geração dos pares de chaves da SISP Root CA é processada de acordo com os requisitos e algoritmos definidos nesta política.

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

O hardware criptográfico, usado para a geração de chaves da SISP Root CA, cumpre os requisitos FIPS 140-2 nível 3 e/ou Common Criteria EAL 4+ e, efetua a manutenção de chaves, armazenamento e todas as operações que envolvem chaves criptográficas utilizando exclusivamente o hardware. O acesso a chaves críticas é protegido por políticas de segurança, divisão de papéis entre os Grupos de Trabalho, assim como através de regras de acesso limitado de utilizadores. As cópias de segurança de chaves criptográficas são efetuadas apenas usando hardware, permitindo que estas cópias sejam devidamente auditadas e que na eventualidade de uma perca de dados, possa haver uma recuperação total e segura das chaves.

A geração do par de chaves da SISP Root CA é efetuada por elementos autorizados dos Grupos de trabalho num hardware criptográfico que cumpre os requisitos FIPS 140-2 nível 3 e/ou Common Criteria EAL 4+.

O funcionamento da SISP Root CA é efetuado em modo offline e o certificado é assinado pela ECR-CV.

8.1.2 ENTREGA DA CHAVE PRIVADA À EC SUBORDINADA

A SISP Root CA não gera a chave privada associada aos certificados que emite.

8.1.3 ENTREGA DA CHAVE PÚBLICA AO EMISSOR DO CERTIFICADO

A chave pública é entregue à SISP Root CA, de acordo com os procedimentos indicados na secção 6.2.2.

8.1.4 ENTREGA DA CHAVE PÚBLICA DA EC ÀS PARTES CONFIANTES

A chave pública da SISP Root CA será disponibilizada através do certificado da SISP Root CA, conforme secção 6.3.2.

8.1.5 DIMENSÃO DAS CHAVES

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

- 4096 bits RSA para a chave da SISP Root CA.

8.1.6 GERAÇÃO DOS PARÂMETROS DA CHAVE PÚBLICA E VERIFICAÇÃO DA QUALIDADE

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

As chaves da EC são geradas com base na utilização de processos aleatórios/pseudo aleatórios descritos no ANSI X9.17 (Anexo C), de acordo com o estipulado nas normas ISO 9564-1 e 11568-5 respectivamente.

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

O campo "keyUsage" dos certificados, utilizado de acordo com o recomendado no RFC 5280, inclui as seguintes utilizações:

- Key Certificate Signature
- CRL Signature

8.2 PROTEÇÃO DA CHAVE PRIVADA E CARATERÍSTICAS DO MÓDULO CRIPTOGRÁFICO

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

8.2.1 NORMAS E MEDIDAS DE SEGURANÇA DO MÓDULO CRIPTOGRÁFICO

Para a geração dos pares de chaves da SISP Root CA assim como para o armazenamento das chaves privadas, a PKI da SISP utiliza módulo criptográfico em hardware que cumpre as seguintes normas:

- Segurança Física
    - Common Criteria EAL 4+ e/ou
    - FIPS 140-2, nível 3
- Autenticação
    - Autenticação dois factores.

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

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

A PKI da SISP implementou um conjunto de mecanismos e técnicas que obrigam à participação de váriosmembros do Grupo de Trabalho para efetuar operações criptográficas sensíveis na EC.

Todas as operações são efetuadas com um mínimo de dois elementos em funções qualificadas dentro da entidade e em tarefa distinta.

Na prática, são empregues nas diversas funções, pelo menos dois elementos (N=2), entre o conjunto total de pessoas com funções atribuídas dentro da entidade (M=staff).

As chaves privadas da PKI da SISP encontram-se na posse de mais que um elemento. Esta é ativada mediante a inicialização do software da EC por meio de uma combinação de operadores da SISP Root CA e administradores do HSM. Este é o único método de activação da chave privada.

8.2.3 RETENÇÃO DA CHAVE PRIVADA (KEY ESCROW)

A SISP Root CA só efetua a retenção da sua chave privada.

8.2.3.1 POLÍTICAS E PRÁTICAS DE RECUPERAÇÃO DE CHAVES

A chave privada da SISP Root CA é armazenada num HSM, sendo efetuada uma cópia de segurança utilizando uma ligação direta hardware a hardware com autenticação de dois fatores e por representantes de diferentes Grupos de Trabalho..

O hardware de segurança com a cópia de segurança da chave privada da SISP Root CA é colocado num cofre seguro em instalações secundárias seguras, e acessível apenas aos membros autorizados dos Grupos de Trabalho.

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

8.2.3.2 POLÍTICAS E PRÁTICAS DE ENCAPSULAMENTO E RECUPERAÇÃO DE CHAVES DE SESSÃO

Nada a assinalar.

8.2.4 CÓPIA DE SEGURANÇA DA CHAVE PRIVADA

A chave privada da SISP Root CA tem pelo menos uma cópia de segurança, com o mesmo nível de segurança que a chave original.

Todas as chaves que tenham sido alvo de cópias de segurança, são arquivadas por um período mínimo de 20 anos após expiração da sua validade.

8.2.5 ARQUIVO DA CHAVE PRIVADA

As chaves privadas da SISP Root CA, alvo de cópias de segurança, são arquivadas conforme identificado na secção 8.2.3.

8.2.6 TRANSFERÊNCIA DA CHAVE PRIVADA PARA/DO MÓDULO CRIPTOGRÁFICO

As chaves privadas da SISP Root CA não são extraíveis a partir do token criptográfico FIPS 140-2 nível 3.

Se for realizada uma cópia de segurança das chaves privadas da SISP Root CA para um outro token criptográfico, essa cópia é efetuada diretamente, hardware para hardware, garantindo o transporte das chaves entre módulos numa transmissão cifrada.

8.2.7 ARMAZENAMENTO DA CHAVE PRIVADA NO MÓDULO CRIPTOGRÁFICO

As chaves privadas da SISP Root CA são armazenadas de forma cifrada nos módulos do hardware criptográfico.

8.2.8 PROCESSO PARA ATIVAÇÃO DA CHAVE PRIVADA

A chave é ativada quando o sistema/aplicação da SISP Root CA é ligada. Esta activação é efectivada quando os administradores de HSM efectuam a autenticação no modulo criptográfico, sendo obrigatorio a autenmticação utilizando dois factores. Para a ativação da chave privada são necessarios que pelo menos duas pessoas estejam autenticadas. Uma vez a chave ativada, esta permanecerá assim até que o processo de desativação seja executado.

8.2.9 PROCESSO PARA DESATIVAÇÃO DA CHAVE PRIVADA

A chave privada da SISP Root CA é desativada quando o sistema da EC é desligado. Uma vez desativada, esta permanecerá inativa até que o processo de ativação seja executado.

8.2.10 PROCESSO PARA DESTRUIÇÃO DA CHAVE PRIVADA

As chaves privadas da SISP Root CA (incluindo as cópias de segurança) são apagadas/destruídas num procedimento devidamente identificado e auditado no mínimo 30 dias após terminada a sua data de validade (ou se revogadas antes deste período).

A PKI da SISP procede à destruição das chaves privadas garantindo que não restarão resíduos destas que possam permitir a sua reconstrução. Para tal, utiliza a função de formatação (inicialização a zeros)

disponibilizada pelo hardware criptográfico ou outros meios apropriados, de forma a garantir a total destruição das chaves privadas da EC.

8.2.11 AVALIAÇÃO/NÍVEL DO MÓDULO CRIPTOGRÁFICO

Descrito na secção 8.2.1.

8.3 OUTROS ASPETOS DA GESTÃO DO PAR DE CHAVES

8.3.1 ARQUIVO DA CHAVE PÚBLICA

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

8.3.2 PERÍODOS DE VALIDADE DO CERTIFICADO E DAS CHAVES

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

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

− O certificado da SISP Root CA tem uma validade de 12 anos, sendo utilizado para assinar certificados durante os seus primeiros 6 anos, sendo reemitido, o mesmo, antes de atingir os 6 anos e 6 meses de validade;

− O certificado das EC´s subordinadas da SISP tem uma validade de 6 anos, sendo utilizado para assinar certificados durante os seus primeiros 3 anos de validade, sendo reemitido após os 3 anos de validade;

- Os certificados de OCSP (Online Certificate Status Protocol) têm uma validade de cinco anos e 4 meses, sendo utilizados durante os seus primeiros quatro anos de validade, sendo reemitido após o quarto mês de validade;

8.4 DADOS DE ATIVAÇÃO

8.4.1 GERAÇÃO E INSTALAÇÃO DOS DADOS DE ATIVAÇÃO

Os dados de ativação necessários para a utilização da chave privada da SISP Root CA são divididos em várias partes (guardadas em chaves PED – pequenos tokens de identificação digital, com o formato de smartcard – identificadoras de diferentes papéis no acesso à HSM), ficando à responsabilidade de diferentes membros do Grupo de Trabalho. As diferentes partes são geradas de acordo com o definido no processo/cerimónia de geração de chaves e obedecem aos requisitos definidos pela norma FIPS 140-2 nível 3.

8.4.2 PROTEÇÃO DOS DADOS DE ATIVAÇÃO

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

As chaves privadas da SISP Root CA são guardadas, de forma cifrada, em token criptográfico.

8.4.3 OUTROS ASPETOS DOS DADOS DE ATIVAÇÃO

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

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

8.5 MEDIDAS DE SEGURANÇA INFORMÁTICAS

8.5.1 REQUISITOS TÉCNICOS ESPECÍFICOS

O acesso aos servidores da SISP Root CA é restrito aos membros dos Grupos de Trabalho com uma razão válida para esse acesso. A SISP Root CA tem um funcionamento offline, sendo desligada no fim de cada emissão de certificado ou de qualquer outra intervenção técnica necessária e que cumpre os requisitos necessários para identificação, autenticação, controlo de acessos, administração, auditorias, reutilização, responsabilidade e recuperação de serviços e troca de informação.

8.5.2 AVALIAÇÃO/NÍVEL DE SEGURANÇA

Os vários sistemas e produtos empregues pela SISP Root CA são fiáveis e protegidos contra modificações. O módulo criptográfico em Hardware da SISP Root CA satisfaz a norma EAL 4+ Common Criteria forInformation Technology Security Evaluation e/ou FIPS 140-2 nível 3.

8.6 CICLO DE VIDA DAS MEDIDAS TÉCNICAS DE SEGURANÇA

8.6.1 MEDIDAS DE DESENVOLVIMENTO DO SISTEMA

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

É fornecida metodologia auditável que permite verificar que o software da SISP Root CA não foi alterado antes da sua primeira utilização. Toda a configuração e alterações do software são executadas e auditadas por membros dos Grupos de Trabalho da PKI da SISP.

8.6.2 MEDIDAS PARA A GESTÃO DA SEGURANÇA

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

8.6.3 CICLO DE VIDA DAS MEDIDAS DE SEGURANÇA

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

8.7 MEDIDAS DE SEGURANÇA DA REDE

A SISP Root CA, é uma EC off-line sendo que não se encontra ligada a nenhuma rede.

8.8 VALIDAÇÃO CRONOLÓGICA (TIME-STAMPING)

Certificados, CRL's e outras entradas na base de dados contêm sempre informação sobre a data e hora dessa entrada. A informação cronológica não é baseada numa fonte de tempo dedicada. O desvio máximo é de 60 segundos. Todas as operações realizadas na SISP Root CA, e sendo esta EC offline, iniciam-se com a verificação da data/hora do sistema.

9. PERFIL DE CERTIFICADO E CRL

9.1 PERFIL DE CERTIFICADO

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

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

O utilizador de um serviço de segurança que requeira o conhecimento da chave pública do utilizador

necessita, normalmente, de obter e validar o certificado que contém essa chave. Se o serviço não dispuser de uma cópia fidedigna da chave pública da EC que assinou o certificado, assim como do nome da EC e informação relacionada (tal como o período de validade), então poderá ter necessidade de um certificado adicional para obter a chave pública da EC e validar a chave pública do utilizador. Em geral, para validar a chave pública de um utilizador, pode ser necessária uma cadeia de múltiplos certificados, incluindo o certificado da chave pública do utilizador assinado por uma EC e, zero ou mais certificados adicionais de ECs assinados por outras ECs.

O perfil dos certificados emitidos pela SISP Root CA está de acordo com:

- Recomendação ITU.T X.509;
- RFC 5280;
- Legislação nacional aplicável

9.2 PERFIL DA LISTA DE REVOGAÇÃO DE CERTIFICADOS

Quando um certificado é emitido, espera-se que seja utilizado durante todo o seu período de validade. Contudo, várias circunstâncias podem causar que um certificado se torne inválido antes da expiração do seu período de validade. Tais circunstâncias incluem a mudança de nome, mudança de associação entre o titular e os dados do certificado (por exemplo, um trabalhador que termina o emprego) e, o compromisso ou suspeita de compromisso da chave privada correspondente. Sob tais circunstâncias, a EC tem que revogar o certificado.

O protocolo X.509 define um método de revogação do certificado, que envolve a emissão periódica, pela EC, de uma estrutura de dados assinada, a que se dá o nome de Lista de Revogação de Certificados (CRL).

A CRL é uma lista com identificação temporal dos certificados revogados, assinada pela EC e disponibilizada livremente num repositório público. Cada certificado revogado é identificado na CRL pelo seu número de série. Quando uma aplicação utiliza um certificado (por exemplo, para verificar a assinatura digital de um utilizador remoto), a aplicação verifica a assinatura e validade do certificado, assim como obtém a CRL mais recente e verifica se o número de série do certificado não faz parte da mesma. Note-se que uma EC emite uma nova CRL numa base regular periódica.

O perfil da CRL está de acordo com:

- Recomendação ITU.T X.509;
- RFC 5280; e
- Legislação nacional aplicável.

Os perfis das CRL podem ser consultados nos documentos de Políticas de Certificados associadas a esta DPC, relativamente à SISP Root CA.

10. GESTÃO DA POLÍTICA

10.1 PROCEDIMENTO PARA MUDANÇA DE ESPECIFICAÇÕES

10.1.1 PROCEDIMENTO DE ALTERAÇÃO À DPC

10.1.1.1 LISTA DE ALTERAÇÕES

Toda e qualquer alteração que venha a ser realizada à DPC da SISP Root CA será objeto de um documento de proposta de alterações.

10.1.1.2 MECANISMO DE NOTIFICAÇÃO

As alterações às políticas serão disponibilizadas num repositorio e comunicadas às Entidades de Registo.

10.1.1.3 CONTRIBUIÇÕES DOS PARTICIPANTES

As partes confiantes dos serviços prestados pela SISP Root CA (subscritores, entidades de registo, de validação, de timestamping ou mesmo de certificação com as quais estejam estabelecidas relações de confiança mútua) poderão dar contributos e emitir opiniões à SISP ou às Entidades de Registo, pelo email pki@sisp.cv.

10.1.1.4 MECANISMOS PARA TRATAR CONTRIBUTOS

Uma vez compilados, será apresentada uma proposta de alterações formal ao Grupo de Gestão da PKI da SISP, devidamente acompanhada dos contributos recolhidos. O Grupo de Gestão terá como obrigação fazer o pedido de um parecer à Autoridade Credenciadora sobre o impacto destas alterações na credenciação da SISP Root CA.

Uma vez na posse de toda esta informação, o Grupo de Gestão e o Grupo de Trabalho de Segurança deliberarão em relação ao provimento das propostas de alteração da DPC, devendo proceder-se à notificação de todos os interessados sobre as deliberações tomadas. Os subscritores terão então um período máximo de 30 dias para solicitar a rescisão de contrato com a SISP Root CA, sem o qual se tomarão como aceites as novas disposições.

10.1.1.5 PERÍODO DE ENTRADA EM EFEITO DAS ALTERAÇÕES

Após este processo ser concluído as alterações passarão à prática após validação de todos os controlos. Serão adotados procedimentos necessarios para garantir que todas as alterações às PC`s e à DPC são rasteadas e que é adotado um correto mecanismo de controlo de versões.

10.2 POLÍTICAS DE DIVULGAÇÃO E PUBLICAÇÃO

10.2.1 REQUERIMENTO DE DIVULGAÇÃO E PUBLICAÇÃO

Todos os itens constantes das PC`s e da DPC da SISP Root CA estão sujeitos a divulgação e publicação.

Toda a publicação e divulgação serão feitas através do site da SISP (https://pki.sisp.cv/index.html), a não ser que a notificação tenha grande impacto para a SISP e para os titulares/partes confiantes.

A SISP Root CA deve assinar digitalmente cada publicação e cada notificação antes de estas serem colocadas no respetivo repositório.

A SISP disponibilizará, publicará ou notificará os titulares acerca de:

- Formas adequadas de proteção de chaves privadas;
- Riscos associados ao uso de qualquer certificado emitido pela SISP Root CA cuja tecnologia tenha sido descontinuada.
- Regras e praticas de segurança para a utilização dos serviços disponibilizados.

10.2.2 PUBLICAÇÃO DA DPC ATUALIZADA

O documento de DPC, devidamente atualizado está permanentemente disponível através do URL https://pki.sisp.cv/

10.2.3 PROCEDIMENTO DE APROVAÇÃO DA DPC

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

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

11. OUTRAS SITUAÇÕES E ASSUNTOS LEGAIS

Esta secção versa sobre aspetos de negócio e assuntos legais.

11.1 TAXAS

11.1.1 TAXAS POR EMISSÃO OU RENOVAÇÃO DE CERTIFICADOS

Serão disponibilizadas no site da empresa em www.pki.sisp.cv .

11.1.2 TAXAS PARA UTILIZAÇÃO DO CERTIFICADO

Nada a assinalar.

11.1.3 TAXAS PARA ACESSO A INFORMAÇÃO DO ESTADO DO CERTIFICADO OU DE REVOGAÇÃO

O acesso a informação sobre o estado ou revogação dos certificados (CRL) é livre e gratuita.

11.1.4 TAXAS PARA OUTROS SERVIÇOS

As taxas para os serviços de validação cronológica e validação online OCSP são identificadas em proposta formal a efetuar pela SISP.

11.1.5 POLÍTICA DE REEMBOLSO

Nada a assinalar.

11.2 RESPONSABILIDADE FINANCEIRA

11.2.1 SEGURO DE COBERTURA

A SISP dispõe do seguro obrigatório de responsabilidade civil, conforme artigo 45.º do Decreto-Lei n.º 33/2007, de 24 de Setembro.

11.2.2 OUTROS RECURSOS

Nada a assinalar.

11.2.3 SEGURO OU GARANTIA DE COBERTURA PARA TITULARES E PARTES CONFIANTES

A SISP dispõe do seguro obrigatório de responsabilidade civil, conforme artigo 45.º do Decreto-Lei n.º 33/2007, de 24 de Setembro.

11.3 CONFIDENCIALIDADE DA INFORMAÇÃO PROCESSADA

11.3.1 ÂMBITO DA CONFIDENCIALIDADE DA INFORMAÇÃO

Declara-se expressamente como informação confidencial aquela que não poderá ser divulgada a terceiros sem autorização explícita. Esta informação está sob custódia e só os Grupos de Trabalho devidadamente autorizados têm acesso.

11.3.2 INFORMAÇÃO FORA DO ÂMBITO DA CONFIDENCIALIDADE DA INFORMAÇÃO

Considera-se informação de acesso público:

- Política de Certificados;

- Declaração de Práticas de Certificação;
- LCR e,

toda a informação classificada como “pública” (informação não expressamente considerada como “pública” será considerada confidencial).

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

11.3.3 RESPONSABILIDADE DE PROTEÇÃO DA CONFIDENCIALIDADE DA INFORMAÇÃO

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

A coordenação desta responsabilidade é feita pelo CISO. Em caso de quebra de confiança, deverá ser contactado o CISO pelo email ciso@sisp.cv.

11.4 PRIVACIDADE DOS DADOS PESSOAIS

11.4.1 MEDIDAS PARA GARANTIA DA PRIVACIDADE

O Sistema de Gestão de Ciclo de Vida dos Certificados (SGCVC) é responsável pela implementação das medidas que garantem a privacidade dos dados pessoais, de acordo com a legislação caboverdiana.

11.4.2 INFORMAÇÃO PRIVADA

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

11.4.3 INFORMAÇÃO NÃO PROTEGIDA PELA PRIVACIDADE

É considerada informação não protegida pela privacidade, toda a informação fornecida pelo titular e sobre o qual este indica uma opção de processamento.

11.4.4 RESPONSABILIDADE DE PROTEÇÃO DA INFORMAÇÃO PRIVADA

De acordo com a legislação caboverdiana.

11.4.5 NOTIFICAÇÃO E CONSENTIMENTO PARA UTILIZAÇÃO DE INFORMAÇÃO PRIVADA

De acordo com a legislação caboverdiana.

11.4.6 DIVULGAÇÃO RESULTANTE DE PROCESSO JUDICIAL OU ADMINISTRATIVO

Nada a assinalar.

11.4.7 OUTRAS CIRCUNSTÂNCIAS PARA REVELAÇÃO DE INFORMAÇÃO

Nada a assinalar.

11.5 DIREITOS DE PROPRIEDADE INTELECTUAL

Todos os direitos de propriedade intelectual, incluindo os que se referem a certificados, LCR, OID, DPC e PC, bem como qualquer outro documento, propriedade da PKI da SISP pertence à SISP S.A.

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

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

11.6 RENÚNCIA DE GARANTIAS

A PKI da SISP recusa todas as garantias de serviço que não se encontrem vinculadas nas obrigações estabelecidas neste DPC.

11.7 LIMITAÇÕES ÀS OBRIGAÇÕES

A SISP Root CA:

- Responde pelos danos e prejuízos que cause a qualquer pessoa em exercício da sua atividade de acordo com o Artº 62 do DL 33/2007, de 24 de Setembro;
- Responde pelos prejuízos que cause aos titulares ou a terceiros pela falta ou atraso na inclusão no serviço de consulta sobre a vigência dos certificados, da revogação ou suspensão dum certificado, uma vez que tenha conhecimento dele;
- Assume toda a responsabilidade mediante terceiros pela atuação dos titulares das funções necessárias à prestação de serviços de certificação;
- A responsabilidade da administração / gestão da SISP Root CA assenta sobre base objetivas e cobre todo o risco que os particulares sofram sempre que seja consequência do funcionamento normal ou anormal dos seus serviços;
- Só responde pelos danos e prejuízos causados pelo uso indevido do certificado reconhecido, quando não tenha consignado no certificado, de forma clara reconhecida por terceiros o limite quanto ao possível uso;
- Não responde quando o titular superar os limites que figuram no certificado quanto as suas possíveis utilizações, de acordo com as condições estabelecidas e comunicadas ao titular;
- Não assume qualquer responsabilidade no caso de perca ou prejuízo:
    - Dos serviços que prestam, em caso de guerra, desastres naturais ou qualquer outro caso de força maior;
    - Ocasionados pelo uso dos certificados quando excedam os limites estabelecidos pelos mesmo na Politica de Certificados e correspondente DPC;
    - Ocasionado pelo uso indevido ou fraudulento dos certificados ou CRL emitidos pela SISP Root CA.

11.8 INDEMNIZAÇÕES

De acordo com a legislação em vigor.

11.9 TERMO E CESSAÇÃO DA ATIVIDADE

11.9.1 TERMO

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

Esta DPC entra em vigor desde o momento de sua publicação no repositório da SISP Root CA.

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

11.9.2 SUBSTITUIÇÃO E REVOGAÇÃO DA DPC

O Grupo de Trabalho de Gestão pode decidir em favor da eliminação ou emenda de um documento relacionado com a PKI da SISP (incluindo esta DPC) quando:

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

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

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

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

11.10 NOTIFICAÇÃO INDIVIDUAL E COMUNICAÇÃO AOS PARTICIPANTES

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

11.11 ALTERAÇÕES

11.11.1 PROCEDIMENTO PARA ALTERAÇÕES

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

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

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

11.11.2 PRAZO E MECANISMO DE NOTIFICAÇÃO

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

11.11.3 MOTIVOS PARA MUDAR DE OID

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

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

No caso em que o Grupo de Trabalho de Segurança julgue que as alterações à especificação podem afetar a aceitabilidade dos certificados para propósitos específicos proceder-se-á ao aumento do número maior de versão do documento e colocado a zero o número menor da mesma. Também se modificarão os dois últimos números do Identificador de Objeto (OID) que o representa. Este tipo de modificações comunicar-se-á aos utilizadores dos certificados segundo o estabelecido no ponto 11.11.2.

11.12 DISPOSIÇÕES PARA RESOLUÇÃO DE CONFLITOS

Todas reclamações entre utilizadores e a PKI da SISP deverão ser comunicadas pela parte em disputa à Autoridade Credenciadora, com o fim de tentar resolvê-lo entre as mesmas partes.

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

11.13 LEGISLAÇÃO APLICÁVEL

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

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

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

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

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

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

11.14 CONFORMIDADE COM A LEGISLAÇÃO EM VIGOR

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

É responsabilidade da Autoridade Credenciadora zelar pelo cumprimento da legislação aplicável listada na secção 11.13

11.15 PROVIDÊNCIAS VÁRIAS

11.15.1 ACORDO COMPLETO

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

11.15.2 INDEPENDÊNCIA

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

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

11.15.3 SEVERIDADE

Nada a assinalar.

11.15.4 EXECUÇÕES (TAXAS DE ADVOGADOS E DESISTÊNCIA DE DIREITOS)

Nada a assinalar.

11.15.5 FORÇA MAIOR

Nada a assinalar.

11.16 OUTRAS PROVIDÊNCIAS

Nada a assinalar.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] ARME, Declaração de Práticas de Certificação da EC Raiz de Cabo Verde.
[2] ARME, Política de Certificados da ICP-CV e Requisitos mínimos de Segurança. [3] Portaria nº 2/2008, de 28 de Janeiro;
[4] Decreto-Lei nº44/2009 de 9 de Novembro;
[5] Decreto Regulamentar nº. 18/2007, de 24 de Dezembro; [6] Decreto-Lei nº 33 /2007, de 24 de Setembro;
[7] Portaria nº 4/2008
[8] FIPS 140-2. 1994, Security Requirements for Cryptographic Modules.
[9] ISO/IEC 3166. 1997, Codes for the representation of names and countries and their subdivisions.
[10] ITU-T Recommendation X.509. 1997, (1997 E): Information Technology - Open Systems Interconnection – The Directory: Authentication Framework.
[11] NIST FIPS PUB 180-1. 1995, The Secure Hash Algorithm (SHA-1). National Institute of Standards and Technology, "Secure Hash Standard,", U.S. Department of Commerce.
[12] RFC 1421. 1993, Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures.
[13] RFC 1422. 1993, Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management.
[14] RFC 1423. 1993, Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers.
[15] RFC 1424. 1993, Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services.
[16] RFC 2252. 1997, Lightweight Directory Access Protocol (v3).
[17] RFC 2560. 1999, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP. [18] RFC 2986. 2000, PKCS #10: Certification Request Syntax Specification, version 1.7.
[19] RFC 3161. 2001, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).
[20] RFC 3279. 2002, Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
[21] RFC 5280. 2008, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
[22] RFC 3647. 2003, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.
[23] RFC 4210. 2005, Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP). [24] Política de Certificado da EC Raiz de Cabo Verde
[24] CABForum Baseline Requirements
[25] CABForum-EV-Guidelines –v1.7.0