SOCIEDADE INTERBANCÁRIA E SISTEMAS DE PAGAMENTOS

SISP ROOT CA02 - DPC

Código:	PLRC011
Versão:	01
Data da versão:	14/06/2022
Criado por:	SISP
Aprovado por:	Diretor Geral - Jair Silva
Nível de confidencialidade:	Publico

Histórico das alterações

Data	Versão	Criado por	Descrição da alteração
14/06/2022	01	Ruben Veiga	Criação do documento

Índice

ÍNDICE TABELAS

1. Introdução

- **Âmbito**

O presente documento é uma Declaração de Práticas de Certificado e tem como objetivo informar as práticas gerais de emissão e gestão de certificados, seguidas pela Entidade de Certificação Raíz SISPRootCA02 , enquanto prestador de serviços de confiança qualificados no âmbito do *CAB Forum "Baseline for Issuance and Mangement of Publicly-Trusted Certificates" e eIDAS Regulation No. 910/2014*, no suporte à sua atividade de certificação digital

Este documento pode sofrer atualizações regulares.

- **Público-alvo**

Este documento é público e destina-se a todos quantos se relacionam com a Entidades de Certificação Entidade de Certificação Raíz SISPROOTCA02 doravante designada de SISPROOTCA02.

Os certificados emitidos pela SISPROOTCA02 contêm uma referência à presente DPC, Código de documento nºPLRC00X.01, de modo a permitir que Partes confiantes e outras pessoas interessadas, possam encontrar informação sobre o certificado e sobre a entidade que o emitiu.

- **Estrutura do Documento**

Este documento segue a estrutura definida e proposta pelo grupo de trabalho PKIX do IETF, no documento RFC 3647. Assume-se que o leitor está familiarizado com os conceitos de criptografia, infraestruturas de chaves publicas e assinaturas eletrónicas. Não sendo o caso recomenda-se o estudo prévio dos referidos tópicos para melhor compreensão do conteúdo. O documento está estruturado em 9 capítulos sendo os 7 primeiros reservados aos procedimentos e praticas de certificação utilizadas pela PKI da SISP e os restantes dois dedicados à Auditoria/*Compliance* e questões legais, respetivamente.

1.1. Contexto Geral

Esta DPC especifica os requisitos de segurança, políticas e praticas utilizadas pela SISPROOTCA02 na sua atividade de certificação digital e está de acordo 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,*
c) *eIDAS Regulation No.910/2014*
d) *CA –Browser-Forum Baseline Requirements 1.8.4*
e) *ETSI TS 119 312 - Electronic Signatures and Infrastructures (ESI): Cryptographic Suites*

1.2. Designação e Identificação do Documento

Este documento é uma DPC que é representada num certificado através de um número único designado de "identificador de objeto" (OID), sendo o valor do OID associado a este documento, o 1.3.6.1.4.1.4146.1.60.

Este documento é identificado pelos dados constantes na seguinte tabela:

Tabela 1: Informação do documento

INFORMAÇÃO DO DOCUMENTO	
Nome do Documento	Declaração de Prática de Certificação da SISPROOTCA02
Versão do Documento	Versão 1.0
Estado do Documento	Aprovado
OID	1.3.6.1.4.1.4146.1.60
Data de Emissão	14/06/2022
Validade	13/06/2023
Localização	http://pki.sisp.cv/

São efetuadas atualizações ao documento, sempre que se justificar.

1.2.1. Revisões

Versão	Criação	Aprovação	Motivo da Revisão
1.0	14/06/2022	15/06/22	Criação
	Administrador de Segurança	Grupo de Gestão	
	Ruben Veiga	Jair Silva	

1.2.2. Histórico do documento

Tabela 2: Histórico do documento

Data	Versão	Criado por	Descrição da alteração
14/06/2022	1.0	Ruben Veiga	Criação do documento

1.3.Participantes na Infraestrutura 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:

- SISP *Root Certification Authority 02 (SISP Root CA02)*
- SISP QWAC Certification Authority (SISP QWAC)

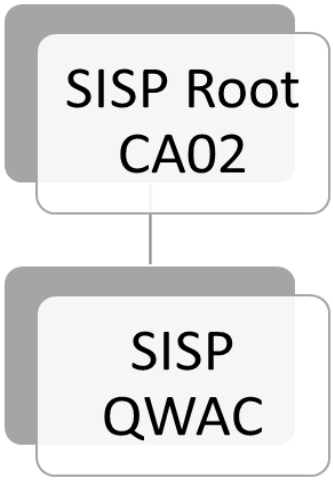

Figura 1: Composição PKI da SISP

1.3.1. Entidades de Certificação

- **SISP Root Certification Authority 02 (SISP Root CA02)**

É uma entidade certificadora de raiz auto-assinada, estando habilitada a emitir certificados para assinatura de entidades certificadoras subordinadas, podendo estas emitir certificados de autenticação web TLS/SSL qualificadas e não qualificadas, e de *code sign*.

Tabela 3: Informação do Certificado (SISP Root CA02)

INFORMAÇÃO DO CERTIFICADO	
Nome Distinto	C = CV, O = SISP, OU = SISP-Sociedade Interbancária e Sistemas de Pagamentos, CN = Entidade de Certificação Raiz da SISP 02
Algoritmo de Assinatura	sha512WithRSAEncryption
Serial Number	6f1566a98112c3fffd6a7b9c0c9bc9d062cf2293
Validade	28 de junho de 2034 06:45:00
Thumbprint	9C:D8:8D:03:09:AB:9F:63:60:73:A3:AA:28:E6:4E:F8:94:CC:A3:E6:D9:37:08:74:BA:ED:C7:1F:C9:3A:2D:1E:DB:80:B3:C8:80:9E:0A:D5:B8:F9:47:2A:A0:51:6C:9B:1E:78:AF:D8:F7:74:97:E9:D7:64:2E:5E:C2:0A:02:62
Emissor	C = CV, O = SISP, OU = SISP-Sociedade Interbancária e Sistemas de Pagamentos, CN = Entidade de Certificação Raiz da SISP 02

- **SISP QWAC *Certification Authority***

É uma entidade certificadora subordinada, assinada pela *SISP Root CA 02*, estando habilitada a emitir certificados para utilizadores finais, de acordo com a *CA/Browser Forum "Baseline for Issuance and Mangement of Publicly-Trusted Certificates" e eIDAS Regulation No. 910/2014*.

A SISP QWAC emite certificados qualificados de Autenticação *Web TLS/SSL Extended Validation(EV*) em conformidade com o *Guidelines for the issuance and management of Extended Validation Certificates da CA/Browser Forum.*

Tabela 4: Informação do certificado (SISP QWAC *Certification Authority*)

INFORMAÇÃO DO CERTIFICADO	
Nome Distinto	C = CV, O = SISP, OU = SISP-Sociedade Interbancaria e Sistemas de Pagamentos, CN= SISP QWAC
Algoritmo de Assinatura	sha512WithRSAEncryption
Serial Number	77a5aacfb1eb23c603e9f429b724826dbc78add6
Validade	29 de junho de 2028 07:22:55
Thumbprint	35:6F:2C:CF:BE:F4:CE:4C:FB:17:21:B8:9D:DB:43:B1:03:F6:AC:18:00:AA:42:49:06:8F:64:3B:1B:EA:AE:9B:F5:DA:7E:10:2C:16:9B:9E:52:CD:8E:31:7D:79:DA:AC:EC:C3:4A:8A:D7:DB:B5:5C:55:15:F3:03:24:FA:7D:5D
Emissor	C = CV, O = SISP, OU = SISP-Sociedade Interbancária e Sistemas de Pagamentos, CN = Entidade de Certificação Raiz da SISP 02

1.3.2. Entidades ou Unidades de Registo

Entidades ou Unidades de Registo são entidades às quais as EC's 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 atuar como Unidade de Registo e/ou estabelecer acordos com entidades terceiras para que estas desempenham este papel.

- **Entidade de Registo Interna**

No âmbito da Entidade de Certificação SISPROOTCA02, a entidade de registo materializa-se pelos serviços internos da PKI da SISP que procedem ao registo e validação dos dados necessários, conforme explicitado na Política de Certificado de cada tipo de certificado emitido.

- **Entidades de Registo Externa**

A hierarquia de confiança da SISPROOTCA02, não dispõe de entidades externas de registo.

1.3.3. Titulares de Certificados

No contexto deste documento o termo subscritor/titular aplica-se a todos os utilizadores finais a quem tenham sido atribuídos certificados pela PKI da SISP.

São considerados titulares de certificados emitidos pela PKI da SISP, aqueles cujo nome está inscrito no campo "Assunto" (*Subject*) do certificado e utilizam o certificado e respetiva chave privada de acordo com o estabelecido nas diversas políticas de certificado descritas neste documento, sendo emitidos certificados para as seguintes categorias titulares:

- Pessoa física ou jurídica;
- Pessoa coletivas (Organizações);
- Serviços (computadores, servidores, domínios, etc.)
- Membros dos grupos de trabalho.

Em alguns casos, os certificados são emitidos diretamente a pessoas física ou jurídica para uso pessoal; no entanto, existem situações em que quem solicita o certificado é diferente do titular do mesmo, por exemplo, uma organização pode solicitar certificados para os seus colaboradores para que estes representem a organização em transações eletrónicas. Nestas situações a entidade que solicita a emissão do certificado é diferente do titular do mesmo.

1.3.4. Partes Confiantes

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

Nesta DPC, considera-se uma parte confiante, aquela que confia no teor, validade e aplicabilidade do certificado emitido na hierarquia de confiança da PKI da SISP.

1.3.5. Outros Participantes

- **Autoridade Supervisora**

A Autoridade Supervisora assume o papel de entidade que disponibiliza serviços de auditoria/inspeção de conformidade, no sentido de aferir se os processos utilizados pela EC nas suas atividades de certificação, estão conformes, de acordo com os requisitos mínimos estabelecidos na legislação e nomas vigentes. Consideram-se como suas principais atribuições as seguintes:

a) Acreditar as entidades de certificação;

b) Auditar as entidades de certificação;

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

d) Zelar pelo adequado funcionamento e eficiente prestação de serviço por parte de entidades de certificação em conformidade com as disposições legais e regulamentares da atividade.

- **Entidades Externas de Prestação de Serviços**

As Entidades que prestam serviços de suporte à PKI da SISP, têm as suas responsabilidades devidamente definidas através de contratos estabelecidos com as mesmas.

- **Auditor de Segurança**

Figura independente do círculo de influência da Entidade de Certificação, exigida pela Autoridade Supervisora. 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 Supervisora.

1.4. Utilização do Certificado

Os certificados emitidos pela SISPROOTCA02 destinam-se em exclusivo para a assinatura de certificados das Entidades Certificadoras de nível imediatamente subsequente ao seu, de sua CRL (Lista de Certificados Revogados) e da sua OCSP, com o objetivo de garantir os seguintes serviços:

- Autenticação;
- Confidencialidade;
- Integridade;
- Privacidade;
- Autenticidade 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. As partes confiantes podem validar a cadeia de confiança e assim garantir a autenticidade e a identidade do titular.

1.4.1. Utilização Adequada do Certificado

Os requisitos e regras definidos neste documento aplicam-se a todos os certificados emitidos pela entidade certificadora SISPROOTCA02.

Os certificados emitidos pela SISPROOTCA02 são também utilizados pelas partes confiantes para verificação da cadeia de confiança, assim como para garantir a autenticidade e identidade do emissor de um certificado de transmissão de dados na web através do protocolo TLS/SSL, a titularidade do domínio, a identidade do website/organização, a confidencialidade e a segurança na troca de informação entre o utilizador e o sítio *web*.

1.4.2. Utilização Não Autorizada

Os certificados emitidos pela SISPROOTCA02 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 atividades de alto risco ou que requeiram uma atividade isenta de falhas, como as relacionadas com o funcionamento de instalações hospitalares, nucleares, controlo de tráfego aéreo, controlo de tráfego ferroviário, ou qualquer outra atividade onde uma falha possa levar à morte, lesões pessoais ou danos graves para o meio ambiente.

1.5.Gestão das Políticas

1.5.1. Organização e Gestão do Documento

A gestão desta DPC é da responsabilidade do Grupo de Trabalho Segurança.

1.5.2. Contactos da Entidade

Tabela 5: Contatos da entidade

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

1.5.3. Entidade que garante a adequação da CPS às políticas

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.

1.5.4. Procedimento para Aprovação da DPC

A validação desta DPC (e/ou respetivas PCs) 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 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.

1.6.Definições e Acrónimos

1.6.1. Definições

Tabela 6: Definições

Definições	
Termo	**Definição**
Assinatura Eletrónica	Dados sob forma eletrónica anexos ou logicamente associados a uma mensagem de dados e que sirvam de método de autenticação.

Assinatura Eletrónica Avançada	Assinatura eletrónica 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 detetar toda e qualquer alteração superveniente do conteúdo deste.
Assinatura Eletrónica Qualificada	Assinatura digital ou outra modalidade de assinatura eletrónica 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 Supervisora	Entidade competente para a credenciação e fiscalização das Entidades de Certificação.
Certificado	Documento eletrónico que liga os dados de verificação de assinatura ao seu titular e confirma a identidade desse titular.
Certificado qualificado	Certificado de assinatura eletrónica, emitido por um prestador de serviços de confiança qualificado, nos termos da legislação de uma determinada jurisdição.
Chave Privada	Elemento do par de chaves assimétricas destinado a ser conhecido apenas pelo seu titular, mediante o qual se apõe a assinatura digital no documento eletrónico, ou se decifra um documento eletrónico previamente cifrado com a Correspondente chave pública.
Chave Pública	Elemento do par de chaves assimétricas destinado a ser divulgado, com o qual se verifica a assinatura digital aposta no documento eletrónico pelo titular do par de chaves assimétricas, ou se cifra um documento eletrónico a transmitir ao titular do mesmo par de chaves.
Credenciação	Ato pelo qual é reconhecido a uma entidade, que o solicite o direito ao exercício de atividade de entidade de certificação credenciada.
Dados de Criação de Assinatura	Um conjunto único de dados, como códigos ou chaves criptográficas privadas, usado pelo signatário para a criação de uma assinatura eletrónica.

Dados Verificação de Assinatura	Um conjunto de dados, como códigos ou chaves criptográficas públicas, usado para verificar a assinatura eletrónica.
Dispositivo de Criação de Assinatura	Suporte lógico ou dispositivo de equipamento utilizado para possibilitar o tratamento dos dados de criação de assinatura.
Dispositivo Seguro de Criação de Assinatura	Dispositivo de criação de assinatura que assegure, através de meios técnicos e processuais adequados, que, i) Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura só possam ocorrer uma única vez e que a confidencialidade desses dados se encontre assegurada; ii) Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura não possam, com um grau razoável de segurança, ser deduzidos de outros dados e que a assinatura esteja protegida contra falsificações realizadas através das tecnologias disponíveis; iii) Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura possam ser eficazmente protegidos pelo titular contra a utilização ilegítima por terceiros; iv) Os dados que careçam de assinatura não sejam modificados e possam ser apresentados ao titular antes do processo de assinatura.
Documento Eletrónico,	Documento elaborado mediante processamento eletrónico de dados.
Endereço Eletrónico	Identificação de um equipamento informático adequado para receber e arquivar documentos eletrónicos.

1.6.2. Acrónimos

Tabela 7: Acrónimos

Acrónimos	
C	*Country*
CN	*Common Name*
CA	*Certification Authority (o mesmo que EC)*
CRL	*Certificate Revocation List (o mesmo que LCR)*
DN	*Distinguished Name*
DPC	Declaração de Prática de Certificação
EC	*Entidade Certificadora*
HSM	*Hardware Security Module*
O	*Organization*
OU	*Organization Unit*
OCSP	*Online Certificate Status Protocol*
OID	*Object Identifier*
LCR	*Lista de Certificados Revogados*
PC	Política de Certificados
PKI	*Public Key Infrastructure*
PKCS	*Public Key Cryptography Standards*
SHA	*Secure Hash Algorithm*

SSl/TLS	*Secure Sockets Layer / Transport Layer Security*
SSCD	*Secure Signature Creation Device*

1.6.3. Referencias bibliográficas

- *RFC 5280: Internet X.509 Public key Infrastructure Certificate and Certificate Revocation List Profile, 2008;*
- *RFC 3647 - Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework, 2003;*
  CA/Browser Forum: Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.8.4;
- *Regulation (EU) No 910/2014;*
- *ETSI TS 119 312: Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.*

2. Responsabilidade de Publicação e Repositório

2.1. Repositórios

A SISP é responsável pelas funções de repositório da SISPROOTCA02, 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.

2.2. Publicação da Informação de Certificação

A SISP mantém um repositório em ambiente Web, permitindo que as Partes Confiantes efetuem 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 para as todas as suas Entidades Certificadoras a seguinte informação pública *on-line* no *URL http://pki.sisp.cv*:

- Certificados das EC's;
- Uma cópia atualizada da DPC das EC's;
- Uma cópia eletrónica atualizada das PC's das EC's;
- Uma relação das EC's vinculadas à cada EC de Raiz;
- Lista de Certificados Revogados das EC's (LCR);
- Uma relação das Entidades de Registos vinculadas e seus respetivos endereços de instalações técnicas em funcionamento;

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

A SISP disponibiliza ainda publicamente e no seu sitio web uma ferramenta que permite aos titulares de certificados web testarem e validarem a cadeia de confiança dos certificados nos estados, validos, revogados e expirados.

2.3. Periodicidade de Publicação

A SISP garante que as atualizações a esta DPC e respetivas políticas serão publicadas sempre que houver necessidade de se proceder a uma alteração. Uma nova CRL da SISPROOTCA02, será publicada, no mínimo, de três em três mês.

2.4. Controlos de Acesso aos Repositórios

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.

3. Identificação e Autenticação

3.1. Atribuição de Nomes

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

- .

3.1.1. Tipos de Nomes

A SISP garante a emissão de certificados contendo um *Distinguished Name (DN) X.509*, definido conforme RFC 5280 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.

O nome único destes certificados está identificado nas respetivas Políticas de Certificados

3.1.2. 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. A SISPROOTCA02 garante que o campo *Common Name* constante do *Suject DN* do certificado é igual a um dos *Subject Alternative Names,* e que foi validado usando pelo menos um dos métodos indicados na secção 3.2.2.4 da *Baseline Requirements CA/B Forum*.

3.1.3. Anonimato ou Pseudónimo de Titulares

Nada a assinalar.

3.1.4. Interpretação de Formato de Nomes

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 exceção dos atributos *country* e *serial number* que são codificados numa *PrintableString.*

3.1.5. Unicidade de 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.

3.1.6. Reconhecimento, Autenticação e Papeis 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.

3.2. Validação de Identidade no Registo Inicial

A SISPROOTCA02 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, os poderes bastantes do representante nomeado pela entidade para a referida emissão.

A emissão de certificados qualificados dentro da hierarquia de confiança da SISP, obriga a que SISPROOTCA02 proceda a um processo rigoroso de verificação da identidade do titular e dos dados a ele associados.

3.2.1. Método de Prova de Posse da Chave Privada

Nos casos em que a SISPROOTCA02 não é a responsável pela geração do par de chaves a ser atribuído ao titular, antes da emissão, deve garantir que o titular está na posse da chave privada correspondente à chave publica incluída no pedido de certificado (CSR).
O método de prova deve ser tanto mais rigoroso quanto maior for a importância e o tipo de certificado solicitado, devendo estar devidamente especificado na Política de Certificado em questão.

3.2.2. Autenticação de Identidade da Organização e Domínio

Os DNs emitidos pela SISPROOTCA02 têm em consideração as marcas registadas, não permitindo a utilização deliberada de nomes registados cuja propriedade não possa ser provada, podendo recusar a emissão do certificado se concluir que outra identificação é mais apropriada.

A SISPROOTCA02 verifica a autenticidade dos dados através de uma das seguintes formas:

a) Por meio de documentos oficiais emitidos por entidades governamentais, designadamente, Certidão Comercial;
b) Autenticação do formulário de pedido de certificado contendo os dados da organização, por uma entidade com poderes para tal (Cartório Notarial, Conservatória, ou outro equivalente);
c) De uma base de dados de terceiros confiável e que seja atualizada periodicamente (D&B, por exemplo);
d) De uma visita ao local, pelo próprio CA ou de um Agente em sua representação;
e) Da prova de controlo do endereço de email sempre que este é incluído no Distinguished Name ou Subject Alternative Name;
f) Da validação do direito de uso e controlo do nome de domínio/endereço constantes do Common Name e Subject Alternative Name do certificado. A SISPROOTCA02 efectua esta validação, utilizando pelo menos um dos métodos descritos na secção 3.2.2.4 da CAB Forum Baseline Requirements.

3.2.2.1. Identidade

Nada a assinalar.

3.2.2.2. Marcas Registadas

Nada a assinalar.

3.2.2.3. Verificação do País

Nada a assinalar.

3.2.2.4. Validação de Autorização ou Controlo de Domínio

Nada a assinalar.

3.2.2.5. Autenticação de um endereço IP

Nada a assinalar.

3.2.2.6. Validação do domínio Wildcard

Nada a assinalar.

3.2.2.7. Exatidão de fontes de dados

Nada a assinalar.

3.2.2.8. Registos CAA

Nada a assinalar.

3.2.3. Autenticação de Identidade do Indivíduo

A verificação de identidade dos titulares e/ou subscritores é feita elo grupo de trabalho de registos e pode ser feita de uma das seguintes vias:

- Mediante a presença física da pessoa singular ou de um representante autorizado da pessoa coletiva, e na presença de dois operadores de registos;
- À distância, utilizando meios de identificação eletrónica, para os quais tenha sido assegurada, antes da emissão do certificado qualificado, a presença física da pessoa singular ou de um representante autorizado da pessoa coletiva e que cumprem os requisitos estabelecidos no artigo 8.o relativamente aos níveis de garantia «substancial» ou «elevado» conforme descrito no Regulamento eIDAS No.910/2024; ou

- Por meio de um certificado de assinatura eletrónica qualificada ou de selo eletrónico qualificado emitidos sob a Infraestrutura de Chave Publica de Cabo Verde (apenas para cidadãos e residentes em Cabo Verde).

3.2.3.1 Identificação de Pessoa Singular

Se o titular é uma pessoa singular, a identidade pode ser verificada através do:

- Nome completo do subscritor
- Data e local de nascimento
- Documento de identificação oficialmente reconhecido pelas autoridades do país
- Documento equivalente á presença física com valor probatório legal.

Se o titular é uma pessoa física em representação de uma pessoa coletiva:

- Nome completo do subscritor
- Data e local de nascimento
- Documento de identificação oficialmente reconhecido pelas autoridades do país
- Documento equivalente à presença física com valor probatório legal
- Designação legal e número de identificação da pessoa coletiva
- Evidencia legal que comprove o poder de representação

Se o titular é uma pessoa singular e é possuidor de uma qualidade profissional:

- Nome completo do subscritor
- Data e local de nascimento
- Documento de identificação oficialmente reconhecido pelas autoridades do país
- Documento equivalente à presença física com valor probatório legal
- Evidencia da profissão exercida
- Número da Licença emitida pela Ordem Profissional
- Área/Departamento a que se encontra afeto

3.2.3.2 Identificação de Pessoa Coletiva

Se o subscritor é uma pessoa coletiva, a identidade pode ser verificada através de:

- Documentos e dados de identificação como sejam:
  - Denominação legal e completa da entidade, p.e, certidão comercial
  - Endereço
  - Número de Identificação Fiscal
  - Número de Registo Comercial

3.2.3.3 Identificação de Dispositivo ou Aplicação

A identificação deve ser autenticada utilizando uma das seguintes provisões:

- Ser oficialmente reconhecido na jurisdição em que o subscritor/titular se encontra registado;
- Pelo nome completo e endereço do subscritor/titular;
- Possuir pelo menos um documento de identificação que contenha fotografia ou
- Número de identificação legal único reconhecido pela jurisdição onde foi emitido.

A SISPROOTCA02 verificará se o candidato tem direito a obter o certificado em questão. Em se tratando de certificados qualificados de autenticação web, a SISPROOTCA02 é obrigada a efetuar a verificação do nome e endereço do representante legal e que a morada da entidade é a que conste dos documentos oficiais ou onde desenvolve a sua atividade.

3.2.4. Informação de Subscritor/Titular Não Verificada

Toda a informação constante do certificado é validada.

3.2.5. Validação de Autoridade

Ver secções 3.2.2 e 3.2.3.

3.2.6. Critérios para Interoperabilidade ou Certificação

Os certificados emitidos pela SISPROOTCA02 são feitos numa hierarquia de confiança. De modo a garantir a total interoperabilidade entre aplicações que usam certificados digitais, recomenda-se o uso exclusivo de caracteres alfanuméricos, sem acentos, espaços, sublinhados, sinal menos, ponto final *([a-z], [A-Z], [0-9], " ", "_", "-", ".")* nas entradas da diretoria X.509.

3.3.Identificação e Autenticação para Renovação de Chaves

3.3.1. Identificação e Autenticação para Renovação de Chaves de Rotina

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

3.3.2. Identificação e Autenticação para Renovação apos 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.

3.4.Identificação e Autenticação para Solicitação de Revogação

O pedido de revogação deve obedecer às condições descritas em pormenor na secção 4.9.

4. Requisitos Operacionais do Ciclo de Vida do Certificado

4.1.Pedido de Certificado

O pedido de certificado deve ser formulado, mediante o preenchimento e assinatura do formulário próprio, disponibilizado pela SISP. A assinatura do formulário pode ser manuscrita ou digital, com recurso a uma assinatura qualificada.

4.1.1. Quem Pode Submeter um Pedido de Certificado

O pedido de certificado pode ser efetuado:

- Pelo representante legal do titular, devidamente mandatado para o efeito, quando o titular é uma pessoa coletiva ou
- Por um representante da SISP.

4.1.2. Processo de Registo e Responsabilidades

Após a receção da documentação inicia-se o processo de validação da autenticidade da documentação e da identidade do titular. Este processo é realizado por dois administradores de registo. Todos os pedidos aceites ou rejeitados serão retidos e preservados pelo período de 7 anos de acordo com a secção 5.5.2 do *CA Browser* Fórum.
A SISPROOTCA02 não dispõe de entidade de registo externa.

4.2.Processamento do Pedido de Certificado

4.2.1. Desempenho de Funções de Identificação e Autenticação

A SISPROOTCA02, assim que rececione o formulário de pedido de emissão de certificado, assim como a informação necessária à emissão do pedido, procederá à validação de toda a informação disponibilizada a fim de verificar a autenticidade dos dados constantes (cf. secção 3.2).

4.2.2. Aprovação ou Rejeição de Pedidos de Certificados

A SISPROOTCA02 apenas aceita o pedido de certificado para emissão se todos os dados constantes no pedido forem autênticos, neste caso sucede-se a aprovação do pedido.

No caso das informações constantes não forem verdadeiras ou forem incompletas, a EC rejeita o pedido de emissão de certificado sendo assim informado ao responsável pelo pedido.

A SISPROOTCA02 não emite certificados para domínios internos.

4.2.3. Prazo para Emissão do Certificado

Nada a assinalar.

4.3.Emissão de Certificados

4.3.1. Ações da CA durante a Emissão do Certificado

A emissão do certificado é efetuada na presença do auditor, por dois membros dos grupos de trabalho, mediante autenticação (cartão+ PIN), sendo um responsável pela inserção dos dados e outro pela validação e aprovação do pedido.

A emissão do certificado resulta da interação com o modulo criptográfico (HSM), seguindo um procedimento específico e de acordo com a política de certificado respetiva. O certificado emitido e assinado pela Entidade Certificadora hierarquicamente superior, é importado na Sub CA correspondente e é gerado a primeira CRL.

A vigência do certificado inicia no momento da sua emissão.

4.3.2. Notificação ao Subscritor/Titular pela CA Emissora do Certificado

Nada a assinalar.

4.4.Aceitação do Certificado

4.4.1. Conduta que Constitui a Aceitação do Certificado

O certificado considera-se aceite após a assinatura do formulário de emissão e aceitação de certificado pelo(s) representante(s) da entidade subordinada.

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.

4.4.2. Publicitação do Certificado pela CA

A SISPROOTCA02 não publicita a lista de certificados emitidos.

4.4.3. Notificação da Emissão de Certificados a Outras Entidades

A SISPROOTCA02 não notifica entidades outras, sobre a sua atividade de emissão de certificados.

4.5.Utilização do Certificado e Par de Chaves

4.5.1. Utilização do Certificado e Par de Chaves pelo Subscritor/Titular

O titular deve utilizar sua chave privada e garantir a proteção dessa chave conforme o previsto nesta DPC.
A sua utilização apenas é permitida:

- A quem for designado como responsável ou representante da entidade requerente no formulário de adesão;
- Após aceitação dos termos e condições de utilização, conforme definido na **secção 4.4.1;**
- Enquanto o certificado se mantiver válido e não estiver na CRL da SISPROOTCA02.

4.5.2. Utilização do Certificado e Chave Pública por Partes Confiantes

As partes confiantes devem usar aplicações/software que estejam em conformidade com o padrão x.509 e devem confiar no certificado apenas se este estiver valido. A SISPROOTCA02 disponibiliza serviços que permitem validar o status do certificado a todo momento e em real time, a saber: OCSP e CRL.

4.6.Renovação de Certificado

A renovação de um certificado é o processo de emissão de um novo certificado com uma nova par de chaves. Pode-se fazer uso dos dados e funções do pedido anterior, desde que estes tenham-se mantido inalterados.

4.6.1. Circunstâncias para a Renovação do Certificado

Nada a assinalar.

4.6.2. Quem pode Solicitar a Renovação de Certificado

Nada a assinalar.

4.6.3. Processamento do Pedido de Renovação de Certificado

Nada a assinalar.

4.6.4. Notificação de Nova Emissão de Renovação de Certificado ao Subscritor/Titular

Nada a assinalar.

4.6.5. Conduta que Constitui a Aceitação de Renovação de Certificado

Nada a assinalar.

4.6.6. Publicitação da Renovação de Certificados pela CA

Nada a assinalar.

4.6.7. Notificação da Renovação de Certificados pela CA a Outras Entidades

Nada a assinalar.

4.7.Re-Key do Certificado

4.7.1. Circunstâncias para o Re-Key de Certificado

A SISPROOTCA02 não suporta o processo Re-Key de certificados

4.7.2. Quem pode Solicitar a Certificação de Uma Nova Chave Publica

Nada a assinalar.

4.7.3. Processamento do Pedido de re-keying

Nada a assinalar.

4.7.4. Notificação de Emissão de Novo Certificado ao Subscritor

Nada a assinalar.

4.7.5. Conduta que Constitui a Aceitação do Certificado Re-Keyed

Nada a assinalar.

4.7.6. Publicitação do Certificado Re-Keyed pela CA

Nada a assinalar.

4.7.7. Notificação do Certificado Re-Keyed pela CA a Outras Entidades

Nada a assinalar.

4.8.Modificação do Certificado

A modificação do certificado é um processo pelo qual o certificado é emitido para um subscritor/titular ou patrocinador mantendo as mesmas chaves, com alterações apenas nas informações do certificado.
A modificação de certificados não é suportada pela SISPROOTCA02.

4.8.1. Circunstâncias para Modificação de Certificado

Nada a assinalar.

4.8.2. Quem Pode Solicitar a Modificação de Certificado

Nada a assinalar.

4.8.3. Processamento do Pedido de Modificação de Certificado

Nada a assinalar.

4.8.4. Notificação de Emissão de Novo Certificado ao Subscritor

Nada a assinalar.

4.8.5. Conduta que Constitui a Aceitação do Certificado Modificado

Nada a assinalar.

4.8.6. Publicitação do Certificado Modificado pela CA

Nada a assinalar.

4.8.7. Notificação do Certificado Modificado pela CA a Outras Entidades

Nada a assinalar.

4.9. Revogação e Suspensão do Certificado

A revogação de certificados é uma ação 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.
A suspensão de certificados não é suportada pela SISPROOTCA02 CA.

4.9.1. Motivos para Revogação

A SISPROOTCA02 deve revogar o certificado no período máximo de 7 dias se ocorrer uma ou mais das seguintes situações:

- A SubCA solicita por escrito a revogação do certificado;
- A SubCA notifica a SISP Root CA2 (Issuing CA) que o pedido inicial de certificado não foi autorizado e não garante autorização retroativamente;
- A Issuing CA obtém evidencia de que a Chave Privada da SubCA correspondente à Chave Publica no certificado foi comprometida ou não cumpre mais os requisitos da Secção 6.1.5 e da Secção 6.1.6;
- A Issuing CA obteve evidencias de que o Certificado foi incorretamente utilizado;
- A Issuing CA é informada de que o Certificado não foi emitido em conformidade ou a SubCA não cumpriu com este documento ou com a Política de Certificados aplicável;
- A Issuing CA determina que uma ou mais informações que aparecem no Certificado é impreciso ou não é verídico;
- A Issuing CA ou a SubCA cessou as operações e não criou condições para que outra CA fornecesse suporte de revogação para o Certificado;
- A revogação é exigida nos termos da Política de Certificação da Issuing CA.

4.9.2. Quem pode solicitar a revogação

Está legitimado para submeter o pedido de revogação, as seguintes entidades:

- A Entidade Certificadora;
- A SISP S.A.;
- A Autoridade Supervisora;

- Uma parte confiante, sempre que demonstre que o certificado foi utilizado com fins diferente dos previstos.

4.9.3. Procedimento para o Pedido de Revogação

Todos os pedidos de revogação devem ser endereçados à SISP S.A. por escrito, através do portal web disponível em https://pki.sisp.cv/ ou por mensagem eletrónica assinada digitalmente, em formulário próprio de pedido de revogação disponibilizado para o efeito.
O pedido é processado nas 24horas seguintes à receção do pedido. Antes de processar o pedido a SISPROOTCA02 obriga-se a verificar a identidade e autenticidade da entidade requerente bem com a manter um registo do pedido após a sua execução.

4.9.4. Período de Carência do Pedido de Revogação

O titular pode solicitar a revogação do certificado a qualquer momento. Contudo recomenda-se em caso de suspeita de comprometimento da chave privada, que o pedido seja feito nas 24 horas seguintes à deteção.

4.9.5. Tempo de Processamento do Pedido de Revogação pela CA

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

4.9.6. Requisito de Verificação da Revogação pelas Partes Confiantes

Antes de utilizarem um certificado, as partes confiantes têm a responsabilidade de verificar o estado do certificado, através da CRL ou num servidor de verificação do estado online (OCSP).

4.9.7. Frequência de Emissão de CRL

A SISPROOTCA02 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 SISPROOTCA02 disponibiliza uma nova CRL a cada **3 meses**.

A CRL pode ser consultada no seguinte repositório: http://crl.sisp.cv/sisprootca02.crl

4.9.8. Latência Máxima para CRL

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

4.9.9. Disponibilidade de Verificação de Estado/Revogação *Online*

A SISPROOTCA02 funciona offline e não dispõe de um serviço de validação de estado de certificado online, OCSP.

4.9.10. Requisitos de Verificação de Revogação *Online*

Antes de fazer uso de um certificado as partes confiantes têm a responsabilidade de verificar o estado de todos os certificados, através da CRL.

A CRL pode ser acedida em https://pki.sisp.cv/document_repository que se encontra disponível 24 horas por dia, 7 dias por semana, excepto durante os períodos de paragem programada para manutenção em que as partes confiantes serão notificadas.

O término de um certificado ocorre quando o prazo de validade expira ou é revogado.

4.9.11. Outras Formas Disponíveis de Anunciar a Revogação

Nada a assinalar.

4.9.12. Requisitos Especiais Relacionados com o Comprometimento de Chave

Complementarmente ás razões mencionadas na secção 4.9.1 desta DPC (Declaração de Praticas de Certificação), as partes podem utilizar o email pki@sisp.cv para reportar o comprometimento ou suspeita de comprometimento da chave privada dos certificados adquiridos.

4.9.13. Circunstâncias para Suspensão

Nada a assinalar.

4.9.14. Quem Pode Solicitar a Suspensão

Nada a assinalar.

4.9.15. Procedimento Para Solicitação de Suspensão

Nada a assinalar.

4.9.16. Limites do Período de Suspensão

Nada a assinalar.

4.10. Serviços de Estado do Certificado

4.10.1. Caraterísticas Operacionais

O *status* dos certificados emitidos encontra-se publicamente disponível através CRL e do serviço OCSP.

4.10.2. Disponibilidade de Serviço

O serviço de *status* do certificado está disponível 24 horas por dia, 7 dias por semana. Se um certificado for revogado, não permanece na CRL após a data de expiração.

4.10.3. Recursos Opcionais

Não estipulado.

4.11. Fim de Subscrição

O término de uma assinatura de certificado ocorre quando o período de validade expira ou o certificado é revogada, de acordo com RFC 3647.

4.12. Custodia e Recuperação de Chaves

4.12.1. Políticas e Praticas de Custodia e Recuperação de Chaves

A SISP retém a chave privada da SISP QWAC e da SISPROOTCA02 e armazena-as em ambiente seguro.

As chaves são encriptadas e armazenadas num HSM e não é possível a sua transferência para outro dispositivo. A SISP dispõe de uma copia de backup das chaves que são armazenadas em local seguro com o mesmo nível de segurança que as originais.

4.12.2. Políticas e Praticas de Encapsulamento e Recuperação de Chave de Sessão

Ver secção 4.12.1

5. Controlos de Segurança Física, 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 políticas seguem as boas práticas recomendadas pelos principais *standards* internacionais relativos à segurança de informação, designadamente ISO 27001.

5.1.Controlos de Segurança Física

5.1.1. 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.

5.1.2. 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.

5.1.3. Energia e Ar Condicionado

O ambiente da 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.

5.1.4. Exposição à Água

Nada a assinalar.

5.1.5. Prevenção e Proteção Contra Incendio

O ambiente da 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.

5.1.6. 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.

5.1.7. 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, etc.) são devidamente limpos de modo a não ser possível recuperar nenhuma informação.

5.1.8. Instalações Externas(alternativas) para Recuperação de Segurança

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

5.2.Medidas de Segurança de 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.

5.2.1. 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

5.2.1.1. Grupo de Auditoria

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

5.2.1.2. 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 atualizadas, 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.

5.2.1.3. 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 afetar a segurança da aplicação.

5.2.1.4. 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.

5.2.1.5. 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.

5.2.2. 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.

5.2.3. Identificação e Autenticação para cada Função

Ver secção 5.2.1.5

5.2.4. 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:

Tabela 8: Funções que requerem separação de responsabilidades

Grupo de Trabalho	Incompatível 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	

5.3. Medidas de Segurança de Pessoal

5.3.1. 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.

5.3.2. Procedimentos de Verificação de Antecedentes

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

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

5.3.3. 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 operacional da 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.

5.3.4. Frequências 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.

5.3.5. Frequências e Sequência da Rotação de Funções

Nada a assinalar.

5.3.6. 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.

5.3.7. Requisitos para Prestadores de Serviços

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

5.3.8. 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.

5.4. Procedimentos de Auditoria de Segurança

5.4.1. Tipo de Eventos Registados

Todos os eventos significativos passiveis de serem auditáveis, devem ser registados, em particular 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.

5.4.2. Frequências de 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, e sempre que haja suspeitas ou atividades anormais ou ameaças de algum tipo. Ações tomadas, baseadas na informação dos registos são também documentadas.

5.4.3. Período de Retenção dos Registos de Auditoria

Os registos estão disponíveis online durante o período de validade da certificação, findo o qual é, são arquivados nos termos descritos na secção 6.5.

5.4.4. 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 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.

5.4.5. Procedimentos para a Copia 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.*

5.4.6. Sistemas 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.

5.4.7. 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.

5.4.8. 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.

5.5.Arquivo de Registos

5.5.1. Tipo de Dados Arquivados

Todos os dados auditáveis são arquivados (conforme indicado na secção 6.4.1), 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 6.4.1 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.

5.5.2. Período de Retenção em Arquivo

Os dados sujeitos a arquivo são retidos pelo período de tempo definido pela legislação nacional ou pelo período de 7 anos conforme recomendação do CAB Fórum, a que for maior.

5.5.3. Proteção dos Arquivos

O arquivo é protegido de modo 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 Política 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.

5.5.4. Procedimentos para as Copias 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*).

5.5.5. 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.

5.5.6. Sistema de Recolha de Dados de Arquivo (Interno/Externo)

Os sistemas de recolha de dados de arquivo são internos.

5.5.7. 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.

5.6. Renovação de Chaves

Nada a assinalar.

5.7.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.

5.7.1. Procedimentos em Caso de Incidente ou Comprometimento

As cópias de segurança das chaves privadas das EC's (geradas e mantidas de acordo com a secção 6.2.3.1) e dos registos arquivados (secção 5.5.1) são guardados em ambientes seguros externos e disponíveis em caso de desastre ou comprometimento. No caso de comprometimento da chave privada da SISPROOTCA02 CA, esta tomará 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.

5.7.2. 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 EC 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.

5.7.3. Procedimentos em Caso de Comprometimento da Chave Privada da Entidade

No caso de a chave privada da EC 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 o *Mozilla Root Repository* e outros repositórios com quem a PKI da SISP tenha estabelecido relações;
- Revogação do certificado da EC e de todos os certificados emitidos no "ramo" da hierarquia de confiança da EC;
- Notificação de todos titulares de certificados emitidos no "ramo" da hierarquia de confiança da EC;
- Geração de novo par de chaves para a EC e inclusão nos vários sistemas/browsers;
- Renovação de todos os certificados emitidos no "ramo" da hierarquia de confiança da EC.

5.7.4. 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.

5.8.Procedimentos em Caso de Extinção da EC ou ER

Em caso de cessação de atividade como prestador de serviços de Certificação, a EC executa os procedimentos previstos no Plano de Cessação de Atividades da PKI da SISP, designadamente:

- Informar o *Mozilla Root Repository* e outros repositórios com quem a PKI da SISP tenha estabelecido relações;
- Revogação de todos os certificados;
- Garantir a transferência, para a sua retenção por outra organização, de toda a informação relacionada com a atividade das EC's;
- Proceder com a destruição de toda a informação classificada ou garantir a sua transferência para sua retenção por outra organização.

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

6. Controlos de Segurança Técnica

Esta secção define as medidas de segurança implementadas pela PKI da SISP para as EC's, de forma a proteger chaves criptográficas geradas por estas, 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.

6.1.Geração e Instalação do Par de Chaves

6.1.1. Geração do Par de Chaves

A geração dos pares de chaves das EC's é processada de acordo com os requisitos e algoritmos definidos nesta política.

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

O hardware criptográfico, usado para a geração de chaves das EC's, 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 chave privada para os certificados de pessoa singular e de pessoa coletiva são gerados pelas EC's, usando hardware criptográfico que cumpre os requisitos FIPS 140-1 nível 3 e/ou *Common Criteria EAL 4+*.

O funcionamento das EC's é efetuado em modo *on-line*.

6.1.2. Entrega da Chave Privada ao Titular

Nada a assinalar.

6.1.3. Entrega da Chave Publica ao Emissor do Certificado

De acordo com os procedimentos indicados secção 4.4.1.

6.1.4. Entrega da Chave Publica da EC às Partes Confiantes

Conforme secção 2.2

6.1.5. 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, segue as recomendações da norma *ETSI TS 119 312 – Electronic Signatures and Infrastructures, Criptographic Suite*, e é a seguinte:

- 4096 bits RSA para a chave das EC's,
- 4096 bits RSA para as chaves associadas aos certificados de utilizadores finais emitidos pela EC, com algoritmo de assinatura sha512RSA.

6.1.6. Geração dos Parâmetros da Chave Publica e Verificação da Qualidade

O processo de geração das chaves é feito diretamente no modulo criptográfico (HSM) e os certificados são assinados pela SISPROOTCA02 que funciona offline.

As chaves da EC são geradas com base na utilização de processos aleatórios/pseudoaleatórios descritos no ANSI X9.17 (Anexo C), de acordo com o estipulado no PKCS#11.

6.1.7. Fins a que se Destinam as Chaves (Campo "*Key Usage" X.509 V3*)

Conforme descrito na secção 1.4.1

6.2. Proteção da Chave Privada e Características do Modulo Criptográfico

Nesta secção são considerados os requisitos para proteção da chave privada e para os módulos criptográficos das EC's. 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 das EC's.

6.2.1. Normas e Medidas de Segurança do Modulo Criptográfico

Para a geração dos pares de chaves das EC's 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 fatores.

6.2.2. Controlo Multi-Pessoal (N de M) para 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 vários membros 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 e administradores do HSM. Este é o único método de ativação da chave privada.

6.2.3. Retenção da Chave Privada (*Key Escrow*)

A SISP só efetua a retenção da sua chave privada.

As chaves privadas das EC's são armazenadas 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 EC é armazenado num cofre seguro em instalações seguras secundárias, e acessível apenas aos membros autorizados dos Grupos de Trabalho. A cópia de segurança da chave privada das EC's 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.

6.2.4. Copia de Segurança da Chave Privada

A chave privada das EC's tem pelo menos uma cópia de segurança, com o mesmo nível de segurança que a chave original.

6.2.5. Arquivo da Chave Privada

As chaves privadas das EC's, alvo de cópias de segurança, são arquivadas conforme identificado na secção 6.2.3.

6.2.6. Transferência da Chave Privada para /do Modulo Criptográfico

As chaves privadas das EC's não são extraíveis do *token* criptográfico FIPS 140-2 nível 3.

Se for realizada uma cópia de segurança das chaves privadas das EC's para um outro *token* criptográfico, essa cópia é efetuada diretamente, *hardware* para hardware, garantindo o transporte das chaves entre módulos numa transmissão cifrada.

6.2.7. Armazenamento da Chave Privada no Modulo Criptográfico

As chaves privadas das EC's são armazenadas de forma cifrada nos módulos do *hardware* criptográfico, conforme descrito na secção 6.2.3.

6.2.8. Ativação da Chave Privada

A SISPROOTCA02 é uma Entidade Certificadora *on-line*, cuja chave privada é ativada quando o sistema da EC é ligado. Esta ativação é efetivada quando os administradores de HSM efetuam a autenticação no módulo criptográfico, sendo obrigatório a autenticação utilizando dois fatores. Para a ativação da chave privada são necessários que pelo menos duas pessoas estejam autenticadas. Uma vez a chave ativada, esta permanecerá assim até que o processo de desativação seja executado.

6.2.9. Desativação da Chave Privada

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

6.2.10. Destruição da Chave Privada

As chaves privadas das EC's (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.

6.2.11. Capacidades do Modulo Criptográfico

Descrito na secção 6.2.1.

6.3. Outros Aspetos da Gestão do par de Chaves

6.3.1. Arquivo da Chave Publica

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

6.3.2. Períodos de Validade do Certificado e das Chaves

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

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

- 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 5 anos e 4 meses, sendo utilizados durante os seus primeiros quatro anos de validade, sendo reemitido após o quarto ano de validade;
- Os certificados para utilizadores finais têm a validade mínima de um ano e máxima de dois anos;

6.4. Dados de Ativação

6.4.1. Geração e Instalação dos Dados de Ativação

Os dados de ativação necessários para a utilização da chave privada das EC's 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.

6.4.2. Proteção dos Dados de Ativação

Os dados de ativação das chaves privadas são guardados em cofres em local seguro.

6.4.3. Outros Aspetos dos Dados de Ativação

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

6.5. Controlos de Segurança Informática

6.5.1. Requisitos Técnicos Específicos

O acesso aos servidores das EC's é restrito aos membros dos Grupos de Trabalho com uma razão válida para esse acesso. As EC's têm funcionamento online, sendo os pedidos de emissão de certificados efetuados a partir do módulo de operação do RA. As EC's e o RA Management dispõem de dispositivos de proteção, designadamente firewall, e que cumpre os requisitos necessários para identificação, autenticação, controlo de acessos, administração, auditorias, reutilização, responsabilidade e recuperação de serviços e troca de informação.

6.5.2. Nível de Segurança Informática

Os vários sistemas e produtos empregues pelas EC's são fiáveis e protegidos contra modificações. O módulo criptográfico em *Hardware* das *Sub CA's* satisfaz a norma *EAL 4+ Common Criteria for Information Technology Security Evaluation e/ou FIPS 140-2* nível 3.

6.6. Ciclo de Vida das Medidas Técnicas de Segurança

6.6.1. 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 das EC's 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.

6.6.2. Medidas de Gestão da Segurança

Todos os sistemas da PKI da SISP estão instalados numa Zona de Alta Segurança. Através dos controlos instalados, é possível garantir a identificação, autenticação e a gestão de todos os acessos.

6.6.3. Ciclo de Vida das Medidas de Segurança

As operações de atualização e manutenção dos produtos e sistemas das EC's, 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.

6.7. Controlos de Segurança da Rede

As EC's dispõem de dispositivos de proteção, nomeadamente sistema firewall, assim como cumpre os requisitos necessários para identificação, autenticação, controlo de acessos, administração, auditorias, reutilização, responsabilidade e recuperação de serviços e troca de informação. Neste sentido, a PKI da SISP que o conjunto de controlos implementados estão em conformidade com todos os requisitos de segurança de rede constantes do "CAB/*Browser Forum – Network and Certificate System Security Requirements*"

6.8. Validação Cronológica (*Time-Stamping*)

Certificados, CRL's e outras entradas na base de dados contêm sempre informação sobre a data e hora dessa entrada. As estas entradas são assinadas digitalmente por um certificado emitido para o efeito. Toda a infraestrutura possui tempo sincronizado através de um NTP com relógio atómico e por duas fontes UTC alternativas:

- Observatório Naval dos Estados Unidos (USNO), Washington DC, USA
- Observatório Real da Bélgica (ORB), Bruxelas, Bélgica
- Real Observatório de La Armada (ROA), Madrid, Espanha

7. Perfis de Certificado, CRL e OCSP

Os perfis de certificados emitidos pela SISPROOTCA02 estão de acordo com a recomendação da ITU.T X.509 versão 3 e atendem aos seguintes standards:

- ETSI EN 319 401 – *General Policy Requirements for Trust Service Providers* e outros relacionados co a prestação de serviços de confiança qualificados;
- *CAB Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates*
- *EU Regulation No.910/2014*
- Legislação nacional

Os perfis dos certificados, podem ser consultadas nos documentos de Políticas de Certificados associadas a esta DPC.

7.1. Perfil do Certificado

7.1.1. Número da Versão

O campo "*version*" do certificado descreve a versão utilizada na codificação do certificado. Neste perfil, a versão utilizada é 3 (três).

7.1.2. Extensões do Certificado

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

7.1.3. OID do Algoritmo

O campo "*signatureAlgorithm*" do certificado contém o OID do algoritmo criptográfico utilizado pela EC para assinar o certificado: *1.2.840.113549.1.1.13 (sha512WithRSAEncryption)*.

7.1.4. Formatos de Nome

Tal como definido na secção 3.1.

7.1.5. Condicionamento nos Nomes

A SISP pode incluir condicionamento aos nomes, no campo "*nameConstraints*" sempre que se justificar.

7.1.6. OID da Política de Certificado

Nada a assinalar.

7.1.7. Utilização de Extensão de Restrições de Política

Nada a assinalar.

7.1.8. Sintaxe e Semânticas de Qualificadores de Política

Nada a assinalar.

7.1.9. Semântica de Processamento para a Extensão critica *Certificate Policies*

Nada a assinalar.

7.2. Perfil 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.

7.2.1. Número(s) de Versão

O campo "*version*" da *CRL* descreve a versão utilizada na codificação da *CRL*. Neste perfil, a versão utilizada é 3 (três).

7.2.2. *CRL* e Extensões da *CRL*

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

7.3. Perfil OCSP

7.3.1. Número(s) de Versão

Nada a assinalar.

7.3.2. Extensões OCSP

Nada a assinalar.

8. Auditoria de Conformidade e Outras Avaliações

8.1. Frequências e circunstâncias de Avaliação

A SISP realiza auditorias regulares, pelo menos uma vez ao ano, e avaliações de conformidade para garantir a conformidade das Entidades Certificadoras integrantes da sua hierarquia de confiança à legislação nacional aplicável, bem como aos padrões internacionais.

As auditorias serão realizadas por entidade externa registada e credenciada para o efeito e os resultados serão comunicados à entidade supervisora.

8.2. Identidade e Qualificações do Auditor

As auditorias serão realizadas por auditor acreditado e habilitado a realizar auditorias provedores de serviços de confiança de acordo com os requisitos previstos no ponto 8.4 *CA-Browser Forum BR 1.8.4*.

8.3. Relação do Auditor com a entidade auditada

O Auditor é uma figura independente, não atuando parcialmente ou discriminatório em relação à entidade sujeita à auditoria. Na relação entre o Auditor e a entidade objeto da auditoria, é assegurada a ausência de qualquer vínculo contratual. O Auditor e a parte auditada não deve ter qualquer relacionamento, atual ou esperado- financeiro, legal, ou de qualquer outra natureza, que possa conduzir a conflito de interesses. Na realização do seu trabalho o Auditor deve atender ao cumprimento do disposto na legislação em vigor nos aspetos relacionados com a proteção de dados pessoais, ao acessar os dados contidos nos arquivos dos titulares de certificados emitidos pela SISPROOTCA02 CA.

8.4. Tópicos cobertos pela auditoria

A auditoria de segurança é realizada com base nos requisitos definidos nesta DPC e de acordo com a legislação nacional aplicável. Tem como objetivo determinar a conformidade dos serviços da SISPROOTCA02 CA com esta declaração de prática e políticas de certificado bem como a adequação em relação a outros documentos,

designadamente políticas relacionadas à segurança logica e física, gestão de serviços de CA, seleção de pessoal, entre outros. Pode ser geral ou parcial, e pode ter incidência em qualquer tipo de documentos / processos.

8.5.Correção de não conformidades

Quando forem detetadas não conformidades em uma auditoria, o Auditor deve:

- Documentar todas as deficiências encontradas durante a auditoria;
- No final do processo de auditoria, reunir com as pessoas responsáveis pela autoridade sob auditoria e apresentar um breve relatório de primeiras impressões;
- Elaborar o relatório de auditoria de acordo com as regras e práticas estabelecidas pela Entidade de Supervisão;
- Submeter o relatório da auditoria à Autoridade auditada;
- A entidade sob auditoria deve apresentar um plano de correção das não conformidades à Entidade de Supervisão, descrevendo ações, metodologia e tempo necessário para a correção das deficiências;

Após análise do plano apresentado, e dependendo do grau de severidade / gravidade

de irregularidades, a Entidade Supervisora deve selecionar uma das três opções seguintes:

- Aceitar os termos, permitindo a continuidade do negócio até a próxima fiscalização;
- Permitir a continuidade dos negócios da autoridade por um período máximo de 90 dias para a correção de irregularidades;
- Cessação imediata de atividades.

8.6.Comunicação de Resultados da Auditoria

Os resultados do processo devem ser comunicados à SISP e à Entidade Supervisora.

8.7.Auditorias Interna

A SISPROOTCA02 realiza periodicamente auditorias internas com o intuito de garantir a qualidade de serviço e a observação da aplicabilidade das normas, políticas e praticas de certificação. Esta auditoria, envolvendo entre 1 a 5% dos certificados emitidos é feita pelo Grupo de Trabalho de Auditoria.

9. Outras Situações e Assuntos Legais

9.1.Taxas

9.1.1. Taxas de emissão ou renovação de certificado

A serem identificadas em proposta formal a efetuar pela SISP.

9.1.2. Taxas de utilização de certificado

Nada a assinalar.

9.1.3. Taxas de 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.

9.1.4. Taxas para outros serviços

Nada a assinalar.

9.1.5. Política de Reembolso

Nada a assinalar.

9.2.Responsabilidade Financeira

9.2.1. 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.

9.2.2. Outros seguros

Nada a assinalar.

9.2.3. Seguro ou garantia de cobertura para titulares

A SISP dispõe do seguro obrigatório de responsabilidade civil, conforme artigo 45.º do Decreto-Lei n.º 33/2007, de 24 de setembro e do ponto 8.4 do *Guidelines for the Issuance and Management of Extended Validation Certificates Version 1.7.6 do CAB Forum.*

9.3.Confidencialidade da informação

9.3.1. 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 devidamente autorizados têm acesso.

9.3.2. Informação fora do âmbito da confidencialidade da informação

Considera-se informação de acesso público:

- Política de Certificados;
- Declaração de Práticas de Certificação;
- CRL e,

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

A SISPROOTCA02 CA permite o acesso a informação não confidencial sem prejuízo de controlos de segurança necessários para proteger a autenticidade e integridade da mesma.

9.3.3. 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.

9.4.Privacidade e Proteção dos Dados Pessoais

9.4.1. Medidas para garantia de privacidade

A SISPROOTCA02 CA é responsável pela implementação das medidas que garantem a privacidade dos dados pessoais, de acordo com a legislação cabo-verdiana.

9.4.2. Informação privada

É considerada informação privada toda a informação fornecida pelo titular e que não seja do domínio publico.

9.4.3. Informação não protegida pela privacidade

É considerada informação não protegida pela privacidade, toda a informação fornecida pelo titular do certificado que seja disponibilizada no certificado digital do titular.

9.4.4. Responsabilidade de proteção da informação privada

De acordo com a legislação cabo-verdiana.

9.4.5. Notificação e consentimento para utilização da informação privada

De acordo com a legislação cabo-verdiana.

9.4.6. Divulgação resultante de processo judicial ou administrativo

Não está prevista a cedência de dados a terceiras partes, exceto em caso de ordem judicial.

9.4.7. Outras circunstâncias para revelação de informação

Não está prevista a cedência de dados a terceiras partes, exceto em caso de ordem judicial.

9.5.Direitos de Propriedade Intelectual

Todos os direitos de propriedade intelectual, incluindo os que se referem a certificados, CRL, OID, DPC e PC, bem como qualquer outro documento, propriedade da SISPROOTCA02 CA 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.

9.6.Obrigações e Garantias

9.6.1. Obrigações e garantias da Entidade Certificadora (CA)

A SISPROOTCA02 CA 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 4.9 deste documento e publicar os certificados revogados na CRL da SISPROOTCA02 CA, com a frequência estipulada na secção 4.9.7;
- 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 Supervisora, 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 6.10.10;
- 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 Supervisora;
- 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.

9.6.2. Obrigações e garantias da entidade de registo

É obrigação das Entidades de Registos:

- Receber os pedidos de emissão de certificados;
- Validar e autenticar os dados dos requerentes de certificados;
- Validar outros dados de requerentes de certificados que se lhes apresentam, cuja verificação é delegada à entidade certificadora para a homologação de certificados com competências

determinadas, como por exemplo, a qualidade de representante de uma pessoa jurídica, qualidade de funcionário de uma organização, qualidade de membro de um grupo profissional, entre outros;
- Remeter os pedidos aprovados para a entidade certificadora a qual se encontra vinculada;
- Receber e validar os pedidos de suspensão ou revogação de certificados e sua remissão à entidade certificadora;
- Colaborar para a realização de inspecções e auditorias por parte da Autoridade Supervisora e seus auditores;
- Garantir a entrega do certificado ao titular do mesmo, ou a quem, legalmente o represente e
- Contratar com os titulares nos termos e modelo definidos pela Entidade Certificadora.

A SISPROOTCA02 CA dispõe única e exclusivamente de Unidades de Registo Internas.

9.6.3. 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 Políticas 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 4.9.1;
- 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.

9.6.4. 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 Política 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.

9.6.5. Obrigações e garantias de outros participantes

Nada a assinalar.

9.7.Renuncia de garantias

A SISPROOTCA02 recusa todas as garantias de serviço que não se encontrem vinculadas nas obrigações estabelecidas nesta DPC.

9.8.Limitações às obrigações

A SISPROOTCA02 é responsável por quaisquer danos causados aos utilizadores finais e terceiros que possam surgir de sua atividade, nos termos da legislação aplicável. Não se responsabiliza por qualquer perda ou danos derivados do uso abusivo ou fora do âmbito do contrato estabelecido com os utilizadores e / ou partes de confiança. A SISPROOTCA02 não assume qualquer responsabilidade em caso de falha dos serviços relacionados com motivos de força maior, como desastres naturais, guerra ou outros semelhantes.

9.9.Indemnizações

De acordo com a legislação em vigor.

9.10. Termo e cessação de atividade

9.10.1. 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 PKI da SISP.

Esta DPC estará em vigor enquanto não for revogada expressamente pela emissão de uma nova versão ou pela renovação das chaves da SISPROOTCA02, momento em que obrigatoriamente se redigirá uma nova versão.

9.10.2. Substituição e revogação

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 pelo período de retenção de dados estipulado pela SISP.

9.11. Notificação individual e comunicação aos participantes

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

9.12. Alterações

9.12.1. 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.

9.12.2. 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

9.12.3. 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 9.12.2.

9.13. Disposições para resolução de conflitos

Todas reclamações entre utilizadores e a PKI da SISP deverão ser comunicadas pela parte em disputa à Autoridade Supervisora, 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, submetem-se à Jurisdição da Comarca da Praia e à lei Cabo-verdiana.

9.14. 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.

9.15. Conformidade com a legislação em vigor

Esta DPC é objeto 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.

Em caso de conflito entre esta DPC e a legislação vigente na jurisdição/país de atuação da CA

tal requisito deve ser reformulado na medida mínima necessária para que seja válido e legal. Isso se aplica apenas a operações ou emissão de certificados que são sujeitos às leis dessa jurisdição. A SISP se compromete a notificar o CAB Fórum sobre os fatos, circunstâncias e leis envolvidas para que possa reavaliar estas Diretrizes adequadamente.

É responsabilidade do Grupo de Trabalho de Gestão zelar pelo cumprimento da legislação aplicável listada na secção 9.14

9.16. Providencias várias

9.16.1. Acordo completo

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

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 do Grupo de Trabalho de Gestão, a avaliação da essencialidade das mesmas.

9.16.2. Cedência de posição

As partes confiantes que operam sob esta DPC ou acordos aplicáveis não podem ceder seus direitos ou obrigações sem o consentimento prévio e escrito da SISP.

9.16.3. Severidade

Nada a assinalar

9.16.4. Execuções (Taxas de advogados e desistência de direitos)

Nada a assinalar

9.16.5. Força maior

As clausulas de força maior constituem parte integrante das Condições Gerais de Emissão do Certificado Digital.

9.17. Outras providencias

Nada a assinalar.

Referências Bibliográficas

- RFC 5280: Internet X.509 Public key Infrastructure Certificate and Certificate Revocation List Profile, 2008;
- RFC 3647 - Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework, 2003;
- CA/Browser Forum: Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.8.4;
- CA/ Browser Forum-EV-Guidelines –v1.7.6;
- Regulation (EU) No 910/2014;
- ETSI 319 412-4 v1.1.1: Electronic Signatures and Infrastructures (ESI); Certificate Profile for Website;
- ETSI 319 412-5 v2.2.3: Electronic Signatures and Infrastructures (ESI); Certificate Profile-QCStatements;
- ETSI TS 119 312: Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.