AUTENTICAÇÃO.GOV
CHAVE MÓVEL DIGITAL

Declaração de Práticas de Operação do SCMD

Políticas (POL#1)

Nível de Acesso: Público

Versão: 3.0

Data: 11/Jan/2019

AMA – Agência para a Modernização Administrativa, I.P.
Rua Abranches Ferrão n.º 10, 3º G 1600-001, Lisboa, Portugal
Telefone: +351 217 231 200 e-mail: ama@ama.pt

Palavras-chave: SCMD, Serviço Chave Móvel Digital, Políticas, Declaração de Práticas de Operação

Autor: AMA - Agência para a Modernização Administrativa, I.P.

Histórico de Versões

Versão	Data	Contribuição
1.0	19/Fev/2018	Versão aprovada do documento.
2.0	22/Mai/2018	Revisão da rastreabilidade para o tempo UTC(k).
3.0	11/Jan/2019	Revisão da DPO, precisando melhor a rastreabilidade para o tempo UTC(k).

Anexos e Documentos Relacionados

Documento	Autor(es)	Descrição
Condições gerais de utilização do serviço SCMD	AMA	Descreve as condições de utilização do serviço SCMD, para aceitação pelo titular do certificado CMD de assinatura qualificada e utilizador do serviço SCMD.
Declaração de Práticas de Certificação da EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão	AMA	Descreve as práticas gerais de emissão e gestão de Certificados seguidas pela Entidade de Certificação Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão (EC CMD) e, explica o que um Certificado fornece e significa, assim como os procedimentos que deverão ser seguidos por Partes Confiantes e por qualquer outra pessoa interessada para confiarem nos Certificados emitidos pela EC CMD.
Política CMD de Assinatura Qualificada	AMA	Política de assinatura qualificada, de acordo com o ETSI TS 119 172 – 1, adaptada ao SCMD.

Estado do documento

Este é um documento controlado e aprovado pela AMA.

Embora este documento possa ser impresso, a versão eletrónica assinada digitalmente pelo(s) elemento(s) do Grupo de Gestão do SCMD, é a cópia controlada. Qualquer cópia impressa deste documento não é controlada.

Sendo um documento **controlado** e de **acesso público**, este documento pode ser arquivado em unidades locais ou de rede, assim como ser acedido diretamente no repositório do SCMD.

Índice

1 Introdução

A Chave Móvel Digital (CMD) surgiu em 2015 como um meio simples e seguro de autenticação dos cidadãos em portais e sítios da Administração Pública na Internet, com dois fatores de segurança: uma palavra-chave e um código recebido por SMS.

Tendo por base a importância da experiência de utilização, conjugado com as novas possibilidades de assinatura eletrónica qualificada "*server-side*" previstas no regulamento europeu 910/2014, o Serviço Chave Móvel Digital (SCMD) é disponibilizado desde a data da sua publicação na *European List of Trusted Lists* (https://webgate.ec.europa.eu/tl-browser/).

Neste contexto, o SCMD gere todos os fluxos de mensagem inerentes ao processo de emissão, ativação e revogação do certificado CMD de assinatura qualificada, assim como da sua utilização para assinatura qualificada "*server-side*" de documentos, de acordo com o número 13 do artigo 2° e o artigo 3° -A da Lei n.° 37/2014, de 26 de junho, republicada com as alterações introduzidas pela Lei 32/2017, de 1 de junho.

Este documento é o documento de Declaração de Práticas de Operação (DPO) do SCMD, e descreve e informa sobre os procedimentos e práticas da assinatura qualificada "*server side*", fornecendo ainda alguns detalhes técnicos, legais e comerciais. Este documento pode sofrer atualizações regulares.

As assinaturas eletrónicas efetuadas pelo SCMD deverão conter uma referência à Política CMD de Assinatura Qualificada, de modo a permitir que partes confiantes e outras pessoas interessadas possam encontrar informação sobre as políticas e práticas seguidas na aposição da assinatura.

Público-Alvo

O público-alvo deste documento são:

- Recursos humanos ao serviço do SCMD,
- Entidades encarregues de auditar o funcionamento do SCMD,
- Utilizadores do SCMD,
- Partes confiantes na assinatura criada pelo SCMD.

Assume-se que o leitor é conhecedor de conceitos básicos de criptografia assimétrica (também denominada de criptografia de chave pública) e de assinatura digital.

1.1 Visão Geral

Um sistema confiável para assinatura "*server-side*" (TW4S – *Trustworthy Systems Supporting Server Signing* – na nomenclatura anglo-saxónica) tem de:

- Estar de acordo com os requisitos do regulamento 910/2014 (eIDAS) para utilização remota de um dispositivo de criação de assinatura, com as chaves privadas de assinatura geridas por um prestador de serviços de confiança;
- Criar uma assinatura digital, sob o controlo exclusivo de uma pessoa física ou de uma pessoa coletiva, que possa ser incorporada numa assinatura eletrónica ou num selo eletrónico conforme definido no regulamento eIDAS.

Para garantir que as assinaturas digitais criadas remotamente ("*server-side*") têm o mesmo reconhecimento jurídico que as assinaturas digitais criadas num ambiente totalmente gerido pelo

titular da chave privada de assinatura (por exemplo, usando cartões inteligentes), o prestador de serviços de assinatura remota (neste caso, o gestor do SCMD) aplica procedimentos específicos de gestão e segurança administrativa e, utiliza sistemas e produtos confiáveis, incluindo canais de comunicação eletrónicos seguros, para garantir que o ambiente de assinatura do servidor é confiável e que as chaves de assinatura são usadas com um alto nível de confiança sob o exclusivo controle do titular das mesmas.

Esta Declaração de Práticas de Operação aplica-se ao SCMD e fornece a informação necessária a todas as partes confiantes para confiarem nas assinaturas criadas pelo SCMD.

A aposição de assinatura eletrónica qualificada pelo SCMD está conforme:

- O artigo 3º-A da Lei n.º 37/2014, de 26 de junho, republicada com as alterações introduzidas pela Lei 32/2017, de 1 de junho;
- O regulamento 910/2014 (eIDAS);
- O despacho 155/2017 (Criação de assinaturas eletrónicas à distância, com gestão por um prestador qualificado de serviços de confiança em nome do signatário), de 5 de Dezembro de 2017, do Gabinete Nacional de Segurança (GNS).

A política associada à aposição de assinatura qualificada a documentos e, as condições de utilização do serviço SCMD, encontram-se descritas nos seguintes documentos de Políticas, de acordo com a seguinte tabela:

OID[1]	Política
2.16.620.2.1.1	Declaração de Práticas de Operação
2.16.620.2.1.2.2	Política CMD de Assinatura Qualificada
2.16.620.2.1.2.3	Condições gerais de utilização do serviço SCMD

1.2 Identificação e Nome do documento

Este documento é a Declaração de Práticas de Operação (DPO) do SCMD e é identificado pelo número único – designado de "identificador de objecto" (OID[1]) – 2.16.620.2.1.1.

Identificação do Documento	
Nome	Declaração de Práticas de Operação
OID	2.16.620.2.1.1
Versão	2.0
Localização	https://www.autenticacao.gov.pt/cmd-assinatura

[1] RFC 3061. 2001. A URN Namespace of Object Identifiers

1.3 Participantes no SCMD

O SCMD gere todos os fluxos de mensagem inerentes ao processo de emissão, ativação e revogação do certificado CMD de assinatura qualificada, assim como da sua utilização para assinatura qualificada "*server-side*" de documentos, de acordo com o ponto 13 do artigo 2º e o artigo 3º -A da Lei n.º 37/2014, de 26 de junho, republicada com as alterações introduzidas pela Lei 32/2017, de 1 de junho.

São participantes no SCMD as seguintes entidades:

- Entidade de Registo – O registo da solicitação de ativação do certificado qualificado CMD para assinatura eletrónica qualificada do cidadão, por cidadão com idade igual ou superior a 16 anos que não se encontre interdito ou inabilitado, é efetuado de acordo com o artigo 2º (Registo) da Portaria CMD[2];
- Entidade de Certificação – A EC CMD, conforme descrito na "Declaração de Práticas de Certificação da EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão", insere-se na hierarquia de confiança do SCEE (Sistema de Certificação Eletrónica do Estado), constituindo-se numa sub-entidade Certificadora do Estado, sendo o seu certificado assinado pela entidade certificadora do Cartão de Cidadão (i.e., por uma Entidade Certificadora do Estado);
- Entidade de geração e guarda de par de chaves – O SCMD efetua a geração e a guarda de par de chaves de assinatura em dispositivo criptográfico seguro, após solicitação de ativação do certificado qualificado CMD à Entidade de Registo, pelo cidadão;
- Entidade de criação de assinatura qualificada – O SCMD disponibiliza ao cidadão um sistema confiável para assinatura "*server-side*" (TW4S) que cria a assinatura qualificada de um documento, sob o controlo exclusivo do titular da chave de assinatura;
- Titular do par de chaves e certificado CMD (também designado por assinante) – Cidadão que ativou o certificado qualificado CMD para assinatura eletrónica qualificada, podendo desse modo assinar documentos com esse certificado através da entidade de criação de assinatura qualificada;
- Parte confiante – Uma parte confiante ou destinatário é uma pessoa singular, entidade ou equipamento que confia na validade dos mecanismos e procedimentos utilizados no processo de emissão do certificado (ou seja, confia que o certificado corresponde na realidade a quem diz pertencer) e no processo de criação da assinatura qualificada (ou seja, confia que a assinatura foi criada pela chave de assinatura do titular do certificado e sob o seu controlo exclusivo).

1.4 Utilização da entidade de criação de assinatura qualificada

1.4.1 Entidade de criação de assinatura qualificada

O sistema confiável para assinatura "*server-side*" (TW4S) devolve, ao assinante ou a uma aplicação, a assinatura digital criada com base nos dados a serem assinados. I.e., o objetivo do TW4S é criar a assinatura digital sob o controlo do titular da chave de assinatura, a partir da representação dos dados a serem assinados (DTBS/R – *Data To Be Signed Representation* – na nomenclatura anglo-saxónica). O TW4S do SCMD é composto por:

[2] Portaria n.º 77/2018 de 16 de Março.

- Aplicação de assinatura em servidor (SSA – *Server Signing Application* – na nomenclatura anglo-saxónica), e
- Dispositivo remoto de criação de assinatura/selo (*remote* SCDev – *Signature/Seal Creation Device* – na nomenclatura anglo-saxónica).

A SSA utiliza o *remote* SCDev para utilizar a chave privada de assinatura, sob o exclusivo controle do titular da mesma. Desse modo, quando a SSA utiliza o *remote* SCDev, o assinante autorizado (i.e., o titular da chave de assinatura) controla remotamente a chave de assinatura com um alto nível de confiança.

O *remote* SCDev é um SCDev aumentado com o módulo de ativação de assinatura (SAM – *Signature Activation Module* – na nomenclatura anglo-saxónica), executado num ambiente protegido contra adulteração (*tamper protected environment*, na nomenclatura anglo-saxónica). Este módulo utiliza os dados de ativação da assinatura (SAD – *Signature Activation Data* – na nomenclatura anglo-saxónica), obtidos de acordo com o protocolo de ativação de assinatura (SAP – *Signature Activation Protocol* – na nomenclatura anglo-saxónica), de modo a garantir um alto nível de confiança de que a chave de assinatura é utilizada sob o controlo exclusivo do titular da mesma.

1.4.2 Utilização

O sistema confiável para assinatura "*server-side*" (TW4S) só pode ser utilizado pelo cidadão, que optar por ativar o certificado qualificado CMD para assinatura eletrónica qualificada de documentos, através de aplicações disponibilizadas e/ou autorizadas pela AMA (indicadas na secção 1.2.1 – Aplicações – no documento "Política CMD de Assinatura Qualificada").

O Cidadão, titular do par de chaves e certificado CMD, é responsável pelo conteúdo do documento que fornece ao TW4S para assinar, sendo a chave de assinatura utilizada sob o controlo exclusivo do titular da mesma.

O TW4S não analisa o documento fornecido para assinar, pelo que a aposição da assinatura não presume concordância com o seu conteúdo.

1.5 Gestão de Políticas

A gestão da Declaração de Práticas de Operação (e Políticas indicadas na secção 1.1) do SCMD é da responsabilidade da AMA (Agência para a Modernização Administrativa, I.P.) e qualquer contacto sobre este assunto deverá ser direcionado para os contactos disponibilizados na página *web* da AMA em www.ama.gov.pt.

O Grupo de Trabalho de Administração de Segurança[3] (GTAS) determina a conformidade e aplicação da DPO (e Políticas). Estes documentos são revistos com uma periodicidade máxima de um ano pelo GTAS e, sempre que houver necessidade de efetuar alterações e/ou correções, novas versões dos documentos são submetidas ao Grupo de Trabalho de Gestão[4] (GTG) para revisão e aprovação. Após a aprovação, as novas versões dos documentos são disponibilizadas publicamente, substituindo a versão anterior.

[3] Ver secção 5.2.1.3.

[4] Ver secção 5.2.1.6.

1.6 Definições e Acrónimos

Termo	Descrição
CMD	Chave Móvel Digital
DPC	Declaração de Práticas de Certificação
DPO	Declaração de Práticas de Operação
DTBS/R	*Data To Be Signed Representation* (representação dos dados a serem assinados)
EC	Entidade de Certificação
GT	Grupo de Trabalho
GTAS	Grupo de Trabalho de Administração de Segurança
GTG	Grupo de Trabalho de Gestão
HSM	*Hardware Security Module* (módulo de segurança em hardware)
NIC	Número de Identificação Civil
Portaria CMD	Portaria n.º 77/2018 de 16 de Março, que regulamenta a Lei 37/2014, de 26 de junho, republicada com as alterações introduzidas pela Lei 32/2017, de 1 de junho
Regulamento 910/2014	Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014 relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno.
Regulamento eIDAS	O mesmo que Regulamento 910/2014.
SAD	*Signature Activation Data* (dados de ativação da assinatura)
SAM	*Signature Activation Module* (módulo de ativação de assinatura)
SAP	*Signature Activation Protocol* (protocolo de ativação de assinatura)
SCA	*Signature Creation Application* (aplicação de criação de assinatura)
SCDev	*Signature/Seal Creation Device* (dispositivo de criação de assinatura/selo eletrónico)
SCEE	Sistema de Certificação Eletrónica do Estado
SCMD	Serviço Chave Móvel Digital
SIC	*Signer's Interaction Component* (componente de interação com o assinante, i.e., o telemóvel/dispositivo do cidadão)
Site CMD	O mesmo que "site SCMD".

Site SCMD	Site do serviço CMD, acessível através de https://www.autenticacao.gov.pt/.
SSA	*Server Signing Application* (Aplicação de assinatura em servidor)
TW4S	*Trustworthy Systems Supporting Server Signing* (sistema confiável para assinatura "*server-side*")

Tabela 1 – Definições e Acrónimos

2 Repositório e Publicação

A AMA é responsável por operar o repositório do SCMD recorrendo aos mecanismos e plataformas tecnológicas mais adequados, assim como por definir a informação a disponibilizar publicamente.

É disponibilizada publicamente no repositório a seguinte informação:

- Cópia eletrónica da "Declaração de Práticas de Operação", "Política CMD de assinatura qualificada" e "Condições gerais de utilização do serviço SCMD", acessíveis a partir do URI https://www.autenticacao.gov.pt/cmd-assinatura;
- Documentos da EC CMD, disponibilizados conforme indicado no documento "Declaração de Práticas de Certificação da EC CMD";
- Outra informação relevante sobre o SCMD é acessível a partir do *site web* SCMD em https://www.autenticacao.gov.pt/cmd-assinatura.

Caso não seja possível obter o certificado da EC CMD ou algum dos certificados da hierarquia de confiança da SCEE, a terceira parte confiante deve assumir que o certificado não está ativo (i.e., não se encontra dentro do seu prazo de validade ou foi revogado). Caso não seja possível obter alguma LCR, a terceira parte confiante deve assumir que todos os certificados emitidos pela EC que assina a LCR não estão ativos (i.e., foram suspensos ou revogados).

A plataforma tecnológica do repositório garante uma disponibilidade de serviço de 99,5%, em período 24hx7d, excluindo manutenções necessárias efetuadas em horário de menor utilização, sendo monitorizada ativamente de modo a poder responder positivamente a todos os pedidos. Toda a informação do repositório é disponibilizada através do protocolo HTTPS (e opcionalmente por HTTP), estando implementados os seguintes mecanismos de segurança:

- Os mecanismos e plataformas tecnológicas utilizadas encontram-se devidamente protegidas, ao nível físico e lógico;
- Os recursos humanos que gerem o repositório têm formação e treino adequado;
- A informação disponibilizada no repositório só pode ser alterada através de processos e procedimentos auditáveis, estando implementados mecanismos de controlo de acesso que impede a alteração por entidades não autorizadas;
- A informação disponibilizada no repositório só pode ser acedida publicamente para leitura.

3 Identificação e Autenticação

Esta secção descreve, de um modo simplificado, o protocolo de ativação de assinatura (SAP) que segue os requisitos do standard CEN 419241-1:2017 (*Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements*) para garantir um alto nível de confiança de que a chave de assinatura é utilizada sob o controlo exclusivo do titular da mesma, no processo de aposição de assinatura qualificada a um documento.

O SAP utilizado no TW4S do SCMD tem os seguintes passos:

1. No *user interface* da SCA – aplicação de criação de assinatura – (site web, aplicação ou *plugin*) no seu ambiente local (PC, portátil ou dispositivo móvel), o cidadão seleciona o(s) documento(s) a assinar e insere a sua informação de autenticação, após o que seleciona a opção de assinatura remota de documento.
2. A SSA:
    a. Valida a informação de autenticação (que será válida durante um período máximo de 5 minutos) e gera um identificador do(s) documento(s) a assinar que devolve para o *user interface* da SCA que a apresenta ao utilizador.
    b. Envia o(s) DTBS/R ao SAM, em conjunto com o NIC e o número de telemóvel do cidadão autenticado (e/ou o identificador único da app/dispositivo).
3. O SAM gera (em HSM) um código de segurança aleatório com um mínimo de 6 dígitos que envia por mensagem SMS (ou por *Push notification*), através do SSA, para o número de telemóvel ou app/dispositivo do cidadão[5] (obtido no passo anterior).
4. O cidadão introduz e envia o código de segurança (recebido por SMS/*Push notification*) através do *user interface* da SCA.
    a. O cidadão deve validar que os dados de identificação do documento, a assinar, recebidos na mensagem SMS/*Push notification*, são os mesmos que lhe são apresentados no *user interface* do SCA, e que o NIC é o seu.
    b. O código de segurança enviado constitui-se como o dado para ativação da assinatura (SAD).
5. A SSA envia o SAD ao SAM.
6. O SAM:
    a. Valida se o *hash* do código de segurança no *SAD* recebido é igual ao *hash* do código de segurança (gerado no passo 3).
    b. Acede à keystore gerida pelo HSM (SCDev) e pede ao HSM (SCDev) para selecionar a chave privada e certificado digital associado ao telemóvel do cidadão, fornecendo a palavra-chave introduzida pelo cidadão através da SCA. O HSM devolve o certificado digital (e toda a hierarquia até à raiz de confiança) e um *handle* para a chave privada no HSM.
    c. Verifica que o certificado digital pertence ao NIC do cidadão e verifica a validade do certificado digital e da hierarquia em que foi emitido. Garante também que o certificado digital foi emitido na hierarquia da EC de Chave Móvel Digital de Assinatura do Cartão de Cidadão.

[5] O telemóvel ou dispositivo do cidadão é designado por componente de interação com o assinante/subscritor do SCMD (ou SIC – *Signer's Interaction Component*).

d. Envia cada DTBS/R e o *handle* ao HSM, que devolve a assinatura qualificada do DTBS/R (efetuada com a chave privada associada ao *handle*).

e. Envia ao HSM um comando para apagar o *handle* e chave privada associada.

f. Devolve à SSA a(s) assinatura(s) qualificada(s) do(s) DTBS/R.

7. A SSA devolve à SCA a(s) assinatura(s) qualificada(s).
8. A SCA pede ao cidadão, através do *user interface*, para indicar onde pretende guardar o(s) documento(s) assinado(s).

3.1 Validação de Identidade no Registo no SCMD

O registo no SCMD corresponde à solicitação de ativação do certificado qualificado CMD para assinatura eletrónica qualificada do cidadão, por cidadão com idade igual ou superior a 16 anos que não se encontre interdito ou inabilitado, de acordo com o artigo 2º (Registo) da Portaria CMD.

O registo no SCMD pode ser presencial ou eletrónico, mas garantindo que a validação inicial da identidade do requerente é sempre feita pelo método de "cara-a-cara".

No caso do registo ser presencial, o funcionário valida pelo método "cara-a-cara", comparando a fotografia no Cartão do Cidadão, Passaporte ou Bilhete de Identidade, com o cidadão na sua presença, confirmando e validando através de reconhecimento facial que o requerente é quem diz ser.

No caso do registo ser eletrónico online, a validação é efetuada com base:

- no certificado de autenticação do Cartão de Cidadão do requerente, tendo previamente sido utilizado o método "cara-a-cara" para emitir o mesmo;
- na Chave Móvel Digital de autenticação, tendo a validação de identidade do registo inicial da mesma sido efetuada pelo método presencial ou pelo método online anterior.

4 Política de Assinatura Qualificada

A política de assinatura qualificada aplica-se a todas as assinaturas qualificadas criadas pelo SCMD, com base na utilização da chave de assinatura sob o exclusivo controle do titular da mesma, com um alto nível de confiança, conforme descrito no documento "Política CMD de Assinatura Qualificada".

5 Controlos Físicos, Operacionais e de Gestão

Os controlos físicos, operacionais e de gestão seguidos pela EC CMD estão descritos no documento "Declaração de Práticas de Certificação da EC CMD" (DPC da EC CMD).

Nesta secção descrevem-se os controlos físicos, operacionais e de gestão implementados pela TW4S e pela Entidade de geração e guarda de par de chaves, que permitem realizar, de modo seguro, as operações necessárias à geração e guarda do par de chaves criptográficos e, à criação de assinatura qualificada "*server-side*". Estes controlos são fundamentais para garantir a confiança no par de chaves gerados assim como no controlo exclusivo da chave de assinatura pelo seu titular.

5.1 Controlos de segurança física

Todos as plataformas tecnológicas e equipamentos utilizados estão situados em Centro de Dados, construídos de forma a proteger fisicamente contra acessos não autorizados e a controlar e auditar o acesso físico a qualquer sistema ou equipamento informático. A arquitetura do Centro de Dados utiliza o conceito de acesso por níveis de segurança, garantindo-se que o acesso a um nível de segurança mais elevado só é possível quando previamente se tenha alcançado os privilégios necessários ao nível imediatamente anterior, nunca sendo possível, em qualquer local do Centro de Dados, aceder ao nível de segurança (n) a partir de outro que não seja o nível (n-1).

As plataformas tecnológicas e equipamentos encontram-se dentro de um bastidor fechado que se situa numa sala do Centro de Dados com controlo de acessos que previne, deteta e impede acessos não autorizados. A sala obedece às seguintes características de construção:

- Parede, teto e pavimento em alvenaria, betão e/ou tijolo;
- Inexistência de janelas;
- Porta(s) de segurança, com chapa em aço, dobradiças fixas e ombreira igualmente em aço, fechadura de segurança acionável eletronicamente, e com características corta – fogo e funcionalidade antipânico.

O perímetro da sala é estanque visto não existirem portas, janelas ou outras brechas não controladas, que possibilitem acessos não autorizados.

O acesso físico à sala passa obrigatoriamente por áreas de controlo humano ou por outros meios de controlo que restringem o acesso físico apenas a pessoal devidamente autorizado. Não é permitida a entrada e permanência na sala a pessoal não autorizado, exceto se forem acompanhados por pessoal devidamente autorizado, sendo nesse caso registado o acesso e motivo, assim como a identificação do pessoal não autorizado e do pessoal autorizado que os acompanha.

O Centro de Dados possui equipamento redundante que garante condições de funcionamento ininterrupto das plataformas tecnológicas e equipamentos:

- Equipamentos de alimentação de energia que garante alimentação contínua ininterrupta durante períodos de falta de corrente, assim como proteção dos equipamentos face a flutuações elétricas que os possam danificar;

- Equipamentos de refrigeração/ventilação/ar condicionado que controlam os níveis de temperatura e humidade, garantindo condições adequadas para o correto funcionamento de todos os equipamentos e plataformas informáticas;
- Equipamentos de deteção de inundação que permitem uma resposta imediata e eficaz em casos de inundação;
- Equipamentos de deteção e alarme de incêndio;
- Equipamentos fixo e móvel de extinção de incêndios, 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.

Adicionalmente, o Centro de Dados tem procedimentos de emergência bem definidos em caso de inundação, incêndio ou outros incidentes, que serão ativados imediatamente de modo a prevenirem e/ou minimizarem o seu impacto.

Toda a informação sensível (dados de produção, informação para auditoria, arquivo ou cópias de segurança) é guardada em cofres (físicos ou digitais) seguros em local externo ao Centro de Dados, com:

- Controlos de acessos físicos e lógicos apropriados para restringir o acesso apenas a pessoal devidamente autorizado;
- Equipamento de alarme, deteção e extinção de incêndios;
- Procedimentos de emergência bem definidos em caso de incidentes, que serão ativados imediatamente de modo a prevenirem e/ou minimizarem o seu impacto, garantindo também a proteção contra danos acidentais.

Quando é necessário transportar fisicamente informação sensível do Centro de Dados para cofres seguros no local externo, o transporte tem de ser efetuado por elemento(s) do Grupo de Trabalho responsável por essa informação.

Sempre que existe necessidade de eliminação de resíduos são seguidas as seguintes regras:

- Documentos em papel que contenham informação sensível são triturados;
- Equipamentos e suportes de armazenamento (discos rígidos, CDs, tokens USB, ...), utilizados para armazenar ou transmitir informação sensível, são limpos de modo a não ser possível recuperar nenhuma informação, através de formatação segura de baixo nível ou destruição física dos equipamentos;
- Equipamentos criptográficos ou chaves físicas de acesso lógico seguem as recomendações do fabricante para eliminação de informação sensível, ou são destruídos fisicamente.

5.2 Controlos procedimentais

Nesta secção são descritas as várias funções necessárias para garantir confiança nos procedimentos (cerimónias, gestão tecnológica, ...) efetuados, assim como as responsabilidades de cada papel, de acordo com as funções identificadas no CEN/TS 419241:2014 (*Security Requirements for Trustworthy Systems Supporting Server Signing*) e CEN 419241-1:2017 (*Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements*).

Como na AMA as tarefas são normalmente efetuadas por equipas/grupos de trabalho, de modo a garantir que mais do que uma pessoa está habilitada a realizar determinada tarefa, os recursos humanos são organizados em Grupos de Trabalho.

Cada Grupo de Trabalho é caracterizado por função e responsabilidade. Os Grupos estão ainda sujeitos a um conjunto de restrições e condições no que concerne à compatibilidade de funções, perfil dos membros, número mínimo de elementos e sua nomeação.

5.2.1 Grupos de Trabalho

Dado os requisitos de segurança inerentes ao funcionamento do SCMD, é vital garantir uma adequada segregação de responsabilidades, de forma a minimizar a importância individual de cada um dos intervenientes e, garantir que o SCMD apenas poderá ser sujeita a ataques do tipo *denial-of-service* mediante o conluio de um número significativo de intervenientes.

5.2.1.1 Grupo de Trabalho de Administração de Sistemas

A função do Grupo de Trabalho de Administração de Sistemas é instalar, configurar e manter os sistemas informáticos, tendo acesso controlado a informação relativa à segurança. Adicionalmente, asseguram a gestão dos Ambientes de Autenticação e de Produção.

As responsabilidades deste grupo são:

- Instalar, configurar e manter os sistemas informáticos do SCMD;
- Gerir o Ambiente de Autenticação e o(s) Ambiente(s) de Produção;
- Manter um inventário atualizado de todos os *tokens* de autenticação (palavra-passe ou *token* físico) usados no Ambiente de Produção e, quando os *tokens* estão à responsabilidade de algum(ns) membro(s) ou Grupo(s) de Trabalho, registar essa informação, guardando esses registos no Ambiente de Autenticação;
- Garantir que cada membro dos vários grupos não detém mais *tokens* de autenticação do que os estritamente necessários à execução das responsabilidades de que está incumbido;
- Registar trocas de palavras-passe de autenticação usadas pelos membros dos grupos;
- Registar a perca de *tokens* de autenticação, descrevendo adequadamente a situação que lhe deu origem;
- Registar sempre que uma palavra-passe de autenticação é comprometida, descrevendo adequadamente a situação que o originou;
- Avaliar os riscos resultantes da perca de um *token* ou o comprometimento de uma palavra-passe de autenticação;
- Tomar medidas ativas de modo a não comprometer o Ambiente de Produção derivado da perca de um *token*, ou do comprometimento de alguma palavra-passe de autenticação.

Os membros deste grupo devem preencher os seguintes requisitos:

- Conhecimentos sólidos de Informática;
- Conhecimentos avançados de redes informáticas, nomeadamente no que concerne à sua arquitetura, administração e securização;

- Conhecimentos sólidos sobre o funcionamento do *hardware* e *software* utilizado pelo SCMD;
- Conhecimentos sólidos sobre normas de segurança da informação, nomeadamente a *ISO/IEC 27002:2013;*
- Fortes competências de organização.

5.2.1.2 Grupo de Trabalho de Operação de Sistemas

A função do Grupo de Trabalho de Operação de Sistemas é operar diariamente os sistemas informáticos, assim como as tarefas de rotina essenciais ao bom funcionamento e operacionalidade do SCMD.

As responsabilidades deste grupo são:

- Operar diariamente os sistemas informáticos do SCMD;
- Monitorizar, reportar e quantificar todos os incidentes e avarias de *software* e *hardware*, despoletando os processos apropriados à correção das mesmas;
- Gerir o Ambiente de Operação;
- Realizar as tarefas de rotina do SCMD, incluindo operações de cópias de segurança e reposição de informação dos seus sistemas.

Os membros deste grupo devem preencher os seguintes requisitos:

- Conhecimentos de Informática, nomeadamente em utilização de sistemas operativos;
- Conhecimentos básicos de redes informáticas, nomeadamente no que concerne à sua interligação física e operação;
- Conhecimentos sólidos sobre o funcionamento do *hardware* e *software* utilizado pelo SCMD.

5.2.1.3 Grupo de Trabalho de Administração de Segurança

A função do Grupo de Trabalho de Administração de Segurança é gerir e implementar as regras, políticas e práticas de segurança, tendo acesso a toda a informação relativa à segurança. Adicionalmente devem propor todas as políticas do SCMD, assegurando que se encontram atualizadas, e garantir que toda a informação indispensável ao funcionamento e auditoria do SCMD se encontra disponível (para elementos devidamente autorizados) ao longo do tempo.

Este grupo tem como responsabilidades:

- Gerir e implementar as regras e práticas de segurança;
- Analisar relatórios de cerimónias e auditorias, propondo ações a tomar ao Grupo de Trabalho de Gestão, caso necessário;
- Definir as regras a serem seguidas pelo Grupo de Trabalho de Custódia, na guarda e disponibilização dos artefactos à sua guarda a membros de outros grupos;
- Gerir o Ambiente de Informação;
- Desencadear e gerir as cerimónias do tipo ad-hoc;
- Definir todas as políticas do SCMD e garantir que se encontram atualizadas e adaptadas à realidade desta;

- Assegurar que as Políticas de Certificados CMD são suportadas pela Declaração de Práticas de Certificação da EC CMD;
- Assegurar que o documento "Política CMD de Assinatura Qualificada" é suportada pela Declaração de Práticas de Operação;
- Propor a atualização dos documentos do SCMD ao Grupo de Trabalho de Gestão, sempre que tal for necessário;
- Assegurar que todos os documentos relevantes e relacionados, direta ou indiretamente, com o funcionamento do SCMD e existentes em formato papel ou eletrónico se encontram atualizados e armazenados no Ambiente de Informação, com o nível de acesso adequado;
- Gerir o Arquivo de Registos (cf. secção 5.5 da Declaração de Práticas de Operação do SCMD).

Os membros deste grupo devem preencher os seguintes requisitos:

- Conhecimentos sólidos sobre Infraestruturas de Chave Pública e Assinatura Eletrónica;
- Conhecimentos básicos sobre o funcionamento do *hardware* e *software* utilizado pelo SCMD;
- Conhecimento avançado sobre o Regulamento 910/2014 (eIDAS) e sobre os standards CEN 419241:2014 (*Security Requirements for Trustworthy Systems Supporting Server*) e CEN 419241-1:2017 (*Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements*);
- Conhecimentos sólidos sobre normas de segurança da informação, nomeadamente a *ISO/IEC 27002:2013*.

5.2.1.4 Grupo de Trabalho de Auditoria de Sistemas

A função do Grupo de Trabalho de Auditoria de Sistemas é efetuar a auditoria interna a todas as ações relevantes e necessárias para assegurar a operacionalidade do SCMD. Estão autorizados a aceder aos arquivos e logs do SCMD com o objetivo de auditar as operações do SCMD, de acordo com a política de segurança.

As responsabilidades deste grupo são:

- Auditar a execução e confirmar a exatidão dos processos e cerimónias do SCMD;
- Aceder aos arquivos de atividade (logs) dos sistemas informáticos do SCMD, para a sua auditoria;
- Registar todas as operações sensíveis;
- Investigar suspeitas de fraudes procedimentais;
- Verificar periodicamente a funcionalidade dos controlos de segurança (lógicos e físicos) existentes nos vários ambientes;
- Registar todos os procedimentos passíveis de auditoria;
- Registar os resultados de todas as ações por si realizadas;
- Validar que todos os recursos usados são seguros;
- Gerir o Ambiente de Auditoria;

- Verificação periódica da integridade dos vários Ambientes, assegurando que lá se encontram os artefactos respetivos[6] e que estão devidamente identificados.

Os membros deste grupo devem preencher os seguintes requisitos:

- Conhecimentos básicos sobre Infraestruturas de Chave Pública e Assinatura Eletrónica;
- Conhecimentos sólidos da documentação do SCMD;
- Conhecimento sobre o Regulamento 910/2014 (eIDAS) e sobre os standards CEN 419241:2014 (*Security Requirements for Trustworthy Systems Supporting Server*) e CEN 419241-1:2017 (*Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements*);
- Conhecimentos sólidos sobre normas de segurança da informação, nomeadamente a *ISO/IEC 27001:2013*.

5.2.1.5 Grupo de Trabalho de Custódia

A função do Grupo de Trabalho de Custódia é efetuar a guarda dos artefactos sensíveis (*tokens* físicos) e artefactos físicos, no Ambiente de Custódia, que podem ser levantados pelos membros de outros grupos, de acordo com as regras definidas pelo Grupo de Trabalho de Administração de Segurança.

As responsabilidades deste grupo são:

- Gerir o Ambiente de Custódia;
- Identificar todos os artefactos à sua guarda;
- Registar os levantamentos e devolução dos artefactos à sua guarda.
- Verificação periódica da integridade dos invólucros dos artefactos à sua guarda.

Os membros deste grupo devem preencher os seguintes requisitos:

- Conhecimentos das regras definidas pelo Grupo de Trabalho de Administração de Segurança, a serem seguidas pelo Grupo de Trabalho de Custódia na guarda e disponibilização dos artefactos a membros de outros grupos.

5.2.1.6 Grupo de Trabalho de Gestão

A função do Grupo de Trabalho de Gestão é a gestão do SCMD, que inclui a nomeação dos membros dos restantes grupos[7].

As responsabilidades deste grupo são:

- Gestão de topo do SCMD;
- Segurança da informação do SCMD;

[6] Caso algum deles se encontre requisitado (quando aplicável), o Grupo de Trabalho de Auditoria deverá verificar se existe registo do seu levantamento e contactar os elementos envolvidos no sentido de confirmar que o têm em seu poder.
[7] À exceção do Grupo de Trabalho de Auditoria de Sistemas.

- Designar os membros dos restantes grupos de trabalho (à exceção do Grupo de Trabalho de Auditoria de Sistemas);
- Rever, analisar e aprovar as políticas e outras propostas efetuadas pelo Grupo de Trabalho de Administração de Segurança;
- Garantir os recursos para a implementação das políticas e propostas aprovadas;
- Autorizar, comunicar e disponibilizar a identificação de todos os indivíduos que pertencem aos vários grupos de trabalho, em um ou mais locais a que esses elementos tenham autorização para aceder.

Os membros deste grupo devem incluir responsáveis seniores da AMA que tenham um bom conhecimento do negócio da empresa, assim como da inserção do SCMD no negócio da AMA.

5.3 Controlos de Segurança de Pessoal

Para que se encontre em condições de pertencer a um dos grupos de trabalho do SCMD, o colaborador (interno ou externo) necessita de satisfazer as seguintes condições:

- Ser formalmente nomeado para o grupo de trabalho;
- Ter recebido treino adequado para a função a desempenhar no grupo de trabalho;
- Fazer prova da sua identidade, usando documentação emitida por fonte fiável;
- Fazer prova de que não se encontra em situação indicadora de inidoneidade;
- Fazer prova de que possui as qualificações e experiência exigidas;
- Não ter conflito de interesses que possa prejudicar a imparcialidade das operações do SCMD;
- Comprometer-se (formalmente) a não revelar (salvo autorização expressa dos representantes legais da AMA) qualquer informação sobre o SCMD, seu funcionamento, sobre os ambientes e recursos humanos ao seu serviço e, sobre a sua operação e funcionamento;
- Comprometer-se (formalmente) a desempenhar as funções para as quais foi nomeado e a não assumir responsabilidades que possam colocar problemas éticos ou deontológicos à sua execução.

A todas as ações não autorizadas (ações que desrespeitem a Declaração de Práticas de Operação, as Políticas ou que não tenham sido aprovadas pelo Grupo de Trabalho de Gestão), realizadas de forma deliberada ou por negligência, são aplicadas sanções de acordo com as regras internas da AMA e das leis de segurança nacional.

5.4 Procedimentos de Auditoria de Segurança

Todos os eventos significativos são auditáveis através de registos eletrónicos ou em papel. Entre esses eventos, incluem-se os eventos específicos indicados na secção 6.2.32, assim como:

- Acesso (ou tentativa) físico à(s) sala(s) e bastidor(es) do Centro(s) de Dados;
- Acesso (ou tentativa) às máquinas do SCMD;
- Solicitação de ativação do certificado qualificado CMD;
- Geração do par de chaves;

- Comunicação (ou tentativa) de emissão, ou revogação de certificados com a EC CMD;
- Criação (ou tentativa) de assinatura qualificada;
- Alteração (ou tentativa) dos parâmetros de segurança do sistema operativo;
- Arranque e paragem de máquinas ou aplicações do SCMD;
- Inicio e fim de sessão em máquinas ou aplicações do SCMD;
- Criar, modificar ou apagar contas do sistema operativo do SCMD;
- Cópia de segurança e recuperação de dados;
- Alterações e atualizações de hardware, sistema operativo e software do SCMD;
- Cerimónias e respetivos procedimentos realizados pelos Grupos de Trabalho;
- Alteração de recursos humanos dos Grupos de Trabalho.

Em geral, as entradas nos registos incluem a seguinte informação/parâmetros (cf. secção 6.2.34):

- Data e hora do evento;
- Identidade do sujeito que causou/registou o evento, quando aplicável;
- Categoria do evento, quando aplicável;
- Descrição do evento (incluindo, sucesso ou falha do evento).

Os registos são analisados, pelo menos, uma vez por ano pelos elementos do grupo de trabalho de Auditoria de Sistemas, e sempre que haja suspeitas de atividades anormais. A análise e eventuais ações recomendadas, baseadas na informação dos registos, são documentadas e fornecidas ao Grupo de Trabalho de Administração de Segurança que será responsável pela sua avaliação e pelos eventuais passos subsequentes que levem à sua concretização.

Os registos eletrónicos são arquivados conforme descrito na secção 5.5. Os registos em papel são digitalizados e arquivados conforme descrito na secção 5.5.

Os registos eletrónicos são protegidos por mecanismos auditáveis que detetam e impedem a sua alteração ou remoção.

Os registos eletrónicos são incluídos nas cópias de segurança, efetuadas para sistemas de armazenamento secundários.

Todos os registos de auditoria, eletrónicos e em papel, são guardados em cofres de segurança do SCMD. Os registos são gerados:

- automaticamente pelos sistemas operativos e aplicações do SCMD,
- automaticamente pelos sistemas de controlo do(s) Centro(s) de Dados onde se encontra o *hardware* do SCMD, e
- manualmente pelos Grupos de Trabalho na execução do trabalho normal de gestão do SCMD ou em cerimónias do SCMD.

O SCMD não notifica o sujeito causador da ocorrência do evento. Baseado no documento de auditoria, o Grupo de Trabalho de Gestão poderá utilizar os meios legais ao dispor da AMA para prosseguir as ações que se considerarem aplicáveis.

Todos os pontos de acesso lógico às máquinas do SCMD estão protegidos, de acordo com mecanismos *state-of-the-art*. Adicionalmente, sempre que é detetado um número anormal de tentativas de acesso, o Grupo de Trabalho de Administração de Sistemas e/ou o Grupo de Trabalho de Operação de Sistemas são automaticamente avisados.

O SCMD é sujeito regularmente a testes de intrusão cujo objetivo é verificar e avaliar proactivamente potenciais vulnerabilidades, de modo a minimizar e eliminar quebras de

segurança. O resultado destes testes é analisado pelo Grupo de Trabalho de Administração de Segurança, que fornece recomendações e/ou um plano de implementação e correção das vulnerabilidades ao Grupo de Trabalho de Gestão, para decisão.

5.5 Arquivo de Registos

Todos os dados auditáveis registados (cf. secção 5.4) são arquivados. Os dados sujeitos a arquivo são arquivados pelo período de tempo definido pela legislação nacional e/ou regulamento 910/2014.

Adicionalmente, são também arquivados:

- Documentos de nomeação dos elementos dos Grupos de Trabalho do SCMD;
- Documentos produzidos nas várias cerimónias;
- Documentos produzidos pelos vários Grupos de Trabalho do SCMD;
- Documentos fornecidos aos Grupos de Trabalho, relevantes para o SCMD (como por exemplo, relatórios de auditorias ou avaliações cf. secção 7);
- Acordos, protocolos e contratos estabelecidos.

Toda a documentação tem origem digital ou, é digitalizada para formato PDF (idealmente, em formato PDF/A[8]) e colocada no cofre digital. Os documentos que tiverem de ser mantidos em formato papel (ou artefactos físicos) são fornecidos, devidamente identificados (e em invólucro lacrado/inviolável, se necessário), ao Grupo de Trabalho de Custódia, para serem guardados em cofre físico.

O cofre digital, onde são arquivados os documentos indicados, é um cofre eletrónico com espaço de armazenamento suficiente para albergar os documentos durante o seu período de retenção, acessível mediante a utilização de uma chave lógica e de um segredo, com características de segurança lógicas apropriadas para resistir a uma tentativa de acesso indevido de considerável intensidade. A sua configuração garante ainda que:

- Apenas membros autorizados dos Grupos de Trabalho têm acesso ao cofre digital;
- Todas as operações efetuadas sobre o cofre digital são auditáveis;
- O cofre digital é protegido contra deterioração de *hardware* (CPU, discos, ...) ao ser disponibilizado em pelo menos duas máquinas virtuais, com as configurações e todos os documentos sincronizados entre as várias maquinas virtuais, garantindo-se também uma migração periódica para novo *hardware*;
- O cofre digital é protegido contra a obsolescência de sistema operativo e aplicações em que está suportado, ao ser garantido que são efetuados os *updates* e *upgrades* indicados pelos fornecedores;
- Os dados arquivados são protegidos contra a obsolescência tecnológica das aplicações que os permitem ler, ao ser garantido que serão guardados em formatos textuais (txt, xml, csv, entre outros) ou em PDF/A.

Cópias de segurança do cofre digital são efetuadas de modo incremental ou total e guardados em dispositivos de memória terciária, em local distinto do centro de dados que alberga o cofre digital.

Todos os documentos colocados no cofre digital têm a indicação da data e hora em que foram criados, não existindo necessidade de validação cronológica mais forte. Note-se, contudo, que

[8] PDF/A é uma versão de PDF especializada para a preservação digital de documentos electrónicos, definida por um standard ISO (ISO 19005).

a data e hora contida nos eventos (cf. secção 5.4) são a data e hora a que esses eventos ocorreram, baseado numa fonte de tempo segura.

5.6 Recuperação em caso de desastre ou comprometimento do SCMD

Esta secção descreve os requisitos relativos a notificação e procedimentos de recuperação em caso de desastre e/ou comprometimento do SCMD.

Em qualquer uma das situações de desastre e/ou comprometimento identificadas, o Grupo de Gestão notifica, sem demora indevida, mas sempre no prazo de 24 horas após ter tomado conhecimento do ocorrido, a entidade supervisora (GNS) e, se necessário, outras entidades, como a autoridade responsável pela proteção de dados (CNPD[9]) e/ou a ANACOM, de todas as violações da segurança ou perdas de integridade que tenham um impacto significativo sobre o serviço de confiança prestado ou sobre os dados pessoais conservados.

5.6.1 Desastre e/ou comprometimento do HSM/SCDev

Um desastre e/ou comprometimento do HSM/SCDev onde estão arquivados os par de chaves à guarda do SCMD leva imediatamente às seguintes ações:

1. Suspensão do serviço de assinatura "server-side" TW4S;
2. Revogação do(s) certificado(s) associado(s) ao(s) par de chaves comprometido(s)/destruído(s) e, eliminação da(s) repetiva(s) chave(s) privada(s) do SCDev caso não tenha(m) sido destruída(s);
3. Informar o(s) titular(es) do(s) certificado(s) e terceiras partes conhecidas, por correio eletrónico e/ou através do site CMD;
4. Auditoria do incidente;
5. Reposição do estado de segurança do HSM/SCDev;
6. Informar o(s) titular(es) do(s) certificado(s) revogado(s) que podem efetuar novo registo no SCMD.

5.6.2 Desastre e/ou comprometimento do TW4S

Um desastre e/ou comprometimento do TW4S leva imediatamente às seguintes ações:

1. Suspensão do serviço de assinatura "server-side" TW4S;
2. Informar os subscritores do serviço de assinatura "server-side", por correio eletrónico e/ou através do site CMD;
3. Auditoria do incidente;
4. Em caso de comprometimento do TW4S, consoante os resultados apurados na auditoria do incidente, serão tomadas as ações mais adequadas – podendo, caso se justifique, ser considerado adicionalmente como um incidente de comprometimento do HSM/SCDev, com as consequências definidas na secção 5.6.1;
5. Reposição do estado de segurança do TW4S;

[9] CNPD – Comissão Nacional de Proteção de Dados

6. Informar os subscritores do serviço de assinatura "server-side" que podem voltar a utilizar o serviço;
7. Reiniciar a disponibilização do serviço de assinatura "server-side" TW4S.

5.6.3 Incidente que corrompa recursos informáticos, *software* e/ou dados

Um incidente que corrompa (ou existir suspeita) recursos informáticos, *software* e/ou dados do SCMD leva imediatamente às seguintes ações:

1. Utilização das cópias de segurança (à exceção do par de chaves geridas pelo HSM/SCDev que não têm cópias de segurança) para verificar a integridade dos dados supostamente corrompidos;
2. Se for confirmado que recursos informáticos, *software* e/ou dados do SCMD estão corrompidos, é suspenso o serviço de assinatura "server-side" TW4S;
3. Informar os subscritores do serviço de assinatura "server-side", por correio eletrónico e/ou através do site CMD;
4. Auditoria do incidente;
5. Se a auditoria não revelar nada mais do que recursos informáticos, *software* e/ou dados do SCMD corrompidos, a recuperação será efetuada com base nas cópias de segurança, reestabelecendo a situação anterior. Caso a auditoria revele comprometimento do HSM/SCDev ou TW4S, atuar-se-á de acordo com as ações definidas para este tipo de incidentes;
6. Informar os subscritores do serviço de assinatura "server-side" que podem voltar a utilizar o serviço;
7. Reiniciar a disponibilização do serviço de assinatura "server-side" TW4S.

5.6.4 Reposição do SCMD

Após um desastre natural ou outro desastre com consequências similares que afetem o Centro de Dados onde estão situadas as plataformas tecnológicas e equipamentos utilizados no SCMD, o serviço SCMD é suspenso, sendo seguidas as ações relativas a incidente de desastre de HSM/SCDev e incidente de desastre de TW4S. O serviço será reposto quando se encontrarem reunidas as condições de segurança e operação necessárias.

5.7 Fim de atividade do SCMD

A atividade do SCMD será terminada em caso de ato administrativo ou legislativo que o imponha. Neste caso, os subscritores do serviço SCMD serão informados através da página do serviço e ser-lhes-á feita uma notificação final 2 (dois) dias antes da cessação formal da atividade. A partir do momento do ato administrativo ou legislativo que determine o fim de atividade do SCMD não serão permitidas novas subscrições no serviço SCMD.
Após o fim da atividade do SCMD, e no mais curto espaço de tempo tecnicamente possível, serão revogados todos os certificados dos subscritores ainda ativos.

Os dados sujeitos a arquivo continuarão arquivados pelo período de tempo definido pela legislação nacional e/ou regulamento 910/2014.

6 Controlos Técnicos de Segurança

Os controlos técnicos de segurança seguidos pela EC CMD estão descritos na DPC da EC CMD.

Nesta secção descrevem-se os controlos técnicos de segurança implementados pela TW4S e pela Entidade de geração e guarda de par de chaves, que estão de acordo com os requisitos do:

- Despacho 155/2017 (Criação de assinaturas eletrónicas à distância, com gestão por um prestador qualificado de serviços de confiança em nome do signatário), de 5 de Dezembro de 2017, do Gabinete Nacional de Segurança (GNS);
- CEN 419241-1:2017 (*Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements*).

6.1 Entidade de geração e guarda de par de chaves

A entidade de geração e guarda de par de chaves aplica procedimentos específicos de gestão e segurança administrativa e, utiliza sistemas e produtos confiáveis, incluindo canais de comunicação eletrónicos seguros, para garantir que o ambiente de geração e guarda de par de chaves é seguro, assim como a comunicação com a Entidade de Certificação CMD e, que o par de chaves é gerado e guardado com um alto nível de confiança sob o exclusivo controle do cidadão titular do par de chaves e certificado CMD.

As operações de geração do par de chaves, emissão do certificado qualificado CMD e guarda inicial do par de chaves constituem-se num processo atómico, na medida em que essas operações são sequenciais e, se alguma delas não for concretizada com êxito, as operações posteriores não são executadas e todas as anteriores são desfeitas.

6.1.1 Geração do par de chaves

A geração do par de chaves criptográficas, associado ao certificado qualificado CMD, é efetuada na solicitação de ativação do certificado qualificado CMD, conforme descrito na secção 3.1, sendo esse par de chaves gerado em *hardware* criptográfico (SCDev/HSM) que cumpre os requisitos FIPS 140-2 nível 3 e/ou *Common Criteria* EAL 4+, não sendo possível extrair o par de chaves desse *hardware* criptográfico. A solicitação de ativação e geração do par de chaves fica registado (cf. secção 5.4).

O comprimento do par de chaves tem em conta:

- Prevenção de possíveis ataques de criptanálise que permitam obter a chave privada durante o seu período de utilização (que corresponde ao período de validade do correspondente certificado);
- Utilização da chave privada para assinatura eletrónica qualificada e validação dos documentos assinados pelas aplicações normalmente disponíveis em ambiente servidor, desktop e *mobile*.

Nessa perspetiva, optou-se por utilizar uma dimensão igual à dimensão das chaves de assinatura qualificada do CC, estabelecendo-se que o comprimento mínimo não será inferior 2048 bits RSA (ou equivalente).

O *hardware* criptográfico utilizado para gerar o par de chaves cumpre com os seguintes requisitos mínimos:

- Certificação *Common Criteria* EAL 4+ e/ou FIPS 140-2 nível 3;

- Geração de números aleatórios – ANSI X9.31 (Anexo A.2.4) ou ANSI X9.62-1998 (Anexo A.4);
- Geração de par de chaves assimétricas – RSA 2048 bits e RSA 4096 bits;
- Algoritmos de *Hash* – SHA-256;
- Assinatura digital – RSA 2048 – 4096 bits e PKCS #1 v1.5 *padding*.

6.1.2 Emissão do certificado qualificado CMD

Após a geração do par de chaves é efetuado o pedido do respetivo certificado qualificado CMD à Entidade de Certificação CMD, através de canal de comunicação e protocolo eletrónico seguro.

O pedido de emissão do certificado qualificado à EC CMD e respetiva resposta fica registado (cf. secção 5.4).

6.1.3 Guarda do par de chaves

A chave privada de assinatura não é entregue ao titular da mesma, ficando o par de chaves guardado em *hardware* criptográfico (SCDev/HSM) que cumpre os requisitos FIPS 140-2 nível 3 e/ou *Common Criteria* EAL 4+.

O SCMD implementou uma combinação de controlos físicos, lógicos e procedimentais, de forma a assegurar a segurança, confidencialidade e integridade das chaves privadas guardadas no *hardware* criptográfico. Entre esses controlos, o cidadão define uma palavra-chave de guarda do par de chaves, que é utilizada pelo *hardware* criptográfico como uma das componentes para proteger o par de chaves.

Não são efetuadas cópias de segurança nem arquivo do par de chaves.

6.1.4 Acesso ao par de chaves

O par de chaves só é acedido através do TW4S – *Trustworthy Systems Supporting Server Signing*, aplicando-se os requisitos e restrições indicadas nas secções 3 e 6.2, garantindo um alto nível de confiança de que a chave de assinatura é utilizada sob o controlo exclusivo do titular da mesma.

O período de utilização das chaves é determinado pelo período de validade do certificado respetivo. Após expiração (ou revogação) do certificado, as chaves cessam permanentemente a sua operacionalidade e são eliminadas do HSM/SCDev, deixando de poder ser utilizadas para os fins previstos indicado no campo *Key Usage* do certificado, de acordo com o perfil de certificado descrito na correspondente Política de Certificados.

6.1.5 Medidas de segurança informáticas

O acesso aos servidores da geração e guarda de chaves é restrito aos membros dos Grupos de Trabalho com uma razão válida para esse acesso. Os servidores da geração e guarda de chaves têm um funcionamento on-line, dispondo de dispositivos de proteção de fronteira, nomeadamente sistema firewall, assim como cumprem os requisitos necessários para identificação, autenticação, controlo de acessos, administração, auditorias, recuperação de serviços e troca de informação.

6.1.6 Ciclo de vida das medidas técnicas de segurança

As aplicações são desenvolvidas e implementadas por terceiros de acordo com as suas metodologias de desenvolvimento, técnicas de implementação, práticas de engenharia de software, gestão de produto e regras de segurança. O SCMD possui as licenças necessárias para utilização dessas aplicações, assim como utiliza procedimentos de instalação das aplicações que permitem verificar que o *software* não foi alterado antes da sua primeira utilização.

Após a instalação do software são utilizados mecanismos para controlar e monitorizar os vários sistemas, assim como são efetuados controlos regulares utilizando ferramentas que asseguram a integridade, segurança e correta operação do software.

As operações de atualização e manutenção dos sistemas de geração e guarda de chaves são efetuadas por elementos do Grupo de Trabalho com adequada formação para o efeito e, de acordo com os procedimentos indicados pelos fornecedores.

6.1.7 Medidas de segurança da rede

Os controlos de segurança da rede de servidores de geração e guarda de chaves dispõem de sistemas ativos de deteção de ataques e intrusão assim como de dispositivos de proteção de fronteira (*firewalls*) com as regras adequadas e continuamente monitorizados. O acesso aos servidores tem restrições adicionais de rede, controlo de acessos, autenticação e autorização.

6.1.8 Fonte de tempo

A informação cronológica, em todos os documentos e registos que necessitem da mesma, é sincronizada com fontes de tempo confiável, garantindo rastreabilidade para o tempo UTC(k) através de um dos laboratórios UTC(k) identificados pelo BIPM (*Bureau International des Poids et Mesures*) na sua Circular T (https://www.bipm.org/en/bipm-services/timescales/time-ftp/Circular-T.html). A sincronização é efetuada pelo protocolo NTP[10] em que o desvio máximo para o UTC[11] é de um segundo, sendo que todas as máquinas da infraestrutura sincronizam com o mesmo servidor NTP. Esta precisão é monitorizada, dando origem a um evento a investigar, sempre que for ultrapassada.

6.2 Trustworthy Systems Supporting Server Signing

Um sistema confiável para assinatura "*server-side*" (TW4S – *Trustworthy Systems Supporting Server Signing* – na nomenclatura anglo-saxónica) tem de:

- Estar de acordo com os requisitos do regulamento 910/2014 (eIDAS) para utilização remota de um dispositivo de criação de assinatura, com as chaves privadas de assinatura geridas por um prestador de serviços de confiança;
- Criar uma assinatura digital, sob o controlo exclusivo de uma pessoa física ou de uma pessoa coletiva, que possa ser incorporada numa assinatura eletrónica ou num selo eletrónico conforme definido no regulamento eIDAS.

Para garantir que as assinaturas digitais criadas remotamente ("*server-side*") têm o mesmo reconhecimento jurídico que as assinaturas digitais criadas num ambiente totalmente gerido pelo

[10] NTP – *Network Time Protocol*, de acordo com RFC 5905 (*Network Time Protocol Version 4: Protocol and Algorithms Specification*)

[11] UTC – *Coordinated Universal Time*

titular da chave privada de assinatura (por exemplo, usando cartões inteligentes), o prestador de serviços de assinatura remota (neste caso, o gestor do SCMD) aplica procedimentos específicos de gestão e segurança administrativa e, utiliza sistemas e produtos confiáveis, incluindo canais de comunicação eletrónicos seguros, para garantir que o ambiente de assinatura do servidor é confiável e que as chaves de assinatura são usadas com um alto nível de confiança sob o exclusivo controle do titular das mesmas.

O sistema confiável para assinatura "*server-side*" (TW4S) devolve, ao assinante ou a uma aplicação, a assinatura digital criada com base nos dados a serem assinados. I.e., o objetivo do TW4S é criar a assinatura digital sob o controlo do titular da chave de assinatura, a partir da representação dos dados a serem assinados (DTBS/R). O TW4S do SCMD é composto por:

- Aplicação de assinatura em servidor (SSA), e
- Dispositivo remoto de criação de assinatura/selo (*remote* SCDev).

A SSA utiliza o *remote* SCDev para utilizar a chave privada de assinatura, sob o exclusivo controle do titular da mesma. Desse modo, quando a SSA utiliza o *remote* SCDev, o assinante autorizado (i.e., o titular da chave de assinatura) controla remotamente a chave de assinatura com um alto nível de confiança.

O *remote* SCDev é um SCDev aumentado com o módulo de ativação de assinatura (SAM), executado num ambiente protegido contra adulteração (*tamper protected environment*). Este módulo utiliza os dados de ativação da assinatura (SAD), obtidos de acordo com o protocolo de ativação de assinatura (SAP – *Signature Activation Protocol*), de modo a garantir um alto nível de confiança de que a chave de assinatura é utilizada sob o controlo exclusivo do titular da mesma.

6.2.1 Controlo exclusivo da chave de assinatura

Conforme descrição do protocolo SAP (secção 3):

- A chave de assinatura é utilizada, com um alto nível de confiança, sob o exclusivo controle do seu titular.
- A utilização autorizada da chave de assinatura pelo seu titular, é garantida pelo módulo de ativação de assinatura (SAM) através dos dados de ativação da assinatura (SAD) fornecidos pelo assinante, de acordo com o protocolo de ativação de assinatura (SAP), de modo a permitir o uso da chave de assinatura correspondente.

6.2.2 Assinatura em lote pelo servidor

O serviço SCMD permite a assinatura de um lote de documentos, sempre que o interface com o utilizador SCA garanta que o assinante escolhe os documentos a assinar e, lhe dê a possibilidade de inspecionar todos esses documentos, antes de iniciar a operação de assinatura.

Desse modo, o assinante tem a possibilidade de inspecionar os documentos antes de os assinar e, tem de autorizar a utilização da chave de assinatura conforme descrito na secção 6.2.1.

6.2.3 Chave de assinatura e módulo criptográfico

No TW4S as chaves de assinatura estão protegidas por um ambiente protegido contra adulteração (*tamper protected environment*).

O SCDev é um módulo criptográfico em *hardware* (HSM) com certificação FIPS 140-2 nível 3 e/ou *Common Criteria* EAL 4+. As chaves privadas só são acedidas em claro pelo HSM. Fora do

HSM estão guardadas numa *keystore* PKCS11 e utilizam o HSM para gerir essa *keystore* numa Base de Dados, localizada fisicamente numa máquina protegida contra adulteração.

6.2.4 Autenticação/meio de identificação eletrónica do assinante

Os requisitos para o registo do assinante e as características do meio de identificação eletrónica estão descritos na secção 6.2.50.

6.2.5 Autenticação/mecanismo de autenticação do assinante

Os requisitos do mecanismo de autenticação estão descritos na secção 6.2.50.

6.2.6 Autenticação do assinante/Objetivo da autenticação

Conforme descrição do protocolo SAP (secção 3):

- O SAD é definido, computado ou resulta de uma interação segura entre o SAM e o SIC através do SSA, para autorizar a operação de assinatura no SCDev, e
- O SAD é transmitido ao SAM através do SSA, de forma a autorizar a operação de assinatura no SCDev para um DTBS/R particular.

6.2.7 Autenticação do assinante/Delegação da autenticação a uma terceira parte

Não se aplica no SCMD, já que o processo de autenticação é feito pelo próprio SCMD.

6.2.8 Dados de ativação da assinatura (SAD)

A utilização do SAD para garantir o controlo sobre a chave de assinatura do assinante é implementada pelo SAM. O SAD contribui para autenticar direta ou indiretamente o assinante.

De acordo com o SAP (secção 3), a autenticação do assinante ocorre antes de se obter o SAD. O SIC recebe um código de segurança por SMS/*Push notification*, constituindo-se esse código de segurança, no SAD.

Aquando do registo do cidadão no serviço CMD (conforme secção 3.1), o cidadão forneceu o seu número de telemóvel, tendo o mesmo sido autenticado através de um código de autenticação enviado por SMS e validado pelo serviço de registo.

A titularidade do dispositivo onde é utilizada a app (para *Push notification*), caso exista, é efetuado após o cidadão se registar no site CMD, através dos seguintes passos:

a) O cidadão faz download da app e instala-a no seu dispositivo;

b) O cidadão identifica-se perante a app com o seu número de telemóvel e PIN CMD;

c) O cidadão recebe um SMS com um código de autenticação;

d) O cidadão introduz esse código de autenticação na app.

6.2.9 Protocolo de ativação da assinatura (SAP)

O SAP (secção 3) inclui as seguintes verificações:

- Autenticação do assinante, na utilização da chave de assinatura;
- Autenticidade do pedido de assinatura com um SAD específico;
- A chave de assinatura é válida e está ativa;
- Comunicação segura de todos os elementos do SAD;
- Certificado associado à chave de assinatura é válido.

6.2.10 Componente de interação com o assinante (SIC)

A componente de interação com o assinante (SIC) é constituída por software e/ou hardware operado no ambiente do assinante e sob o seu controlo exclusivo.

A SIC participa sempre no protocolo SAP com o intuito de autenticar o assinante ou gerar o SAD:

- A SIC pode gerar diretamente o SAD, ou
- A SIC pode ser utilizada para autenticar o assinante, e a informação que identifica o assinante é usada na geração do SAD.

No SCMD, a SIC é:

- o telemóvel do cidadão (mais especificamente, o cartão SIM que recebe o SMS), ou
- a app executada no dispositivo (e.g., tablet, smartphone) do cidadão, que recebe a *Push notification*.

O SAD é constituído pelo SMS/*Push notification* recebido do SAM na SIC, conforme descrição do protocolo SAP (secção 3).

6.2.11 Módulo de ativação de assinatura (SAM)

O SAM é operado num ambiente protegido contra adulteração (*tamper protected environment*), de acordo com requisitos das secções 6.2.12 e 6.2.50 e, estabelece um canal de comunicação seguro com o SCDev.

6.2.12 Ambiente protegido contra adulteração

O ambiente protegido contra adulteração (*tamper protected environment*):

- É operado dentro do ambiente protegido do SCMD e protegido do acesso direto de/à Internet;
- Assegura a integridade do código executado nesse ambiente;
- Protege a ligação entre a chave de assinatura e o assinante (a ligação é criada e verificada quando é necessária para a criação da assinatura).

Adicionalmente,

- O par de chaves é gerado, e a chave privada é utilizada, num ambiente protegido contra adulteração;
- O software do SAM é utilizado num ambiente protegido contra adulteração.

Do ponto de vista físico, o ambiente protegido contra adulteração situa-se num bastidor com chave e selos físicos (que permitem verificar a integridade física do ambiente, num procedimento de inspeção de rotina), no nível 4 de segurança, de acordo com a norma técnica D 02 (Requisitos mínimos de segurança física de instalações de entidades certificadoras) do Gabinete Nacional de Segurança (GNS). O SCDev é um HSM com certificação CC EAL 4+ e/ou FIPS 140-2 level 3 e, o SAM encontra-se num servidor em caixa totalmente fechada, com todas os conectores de entrada selados (à exceção dos que estão em uso que não podem ser alterados sem se quebrarem os selos de segurança) e, com todos os parafusos selados e/ou todos os lados da caixa selados. Existe cabo de rede entre o SCDev e o SAM (conforme requisito na secção 6.2.11) que não pode ser alterado sem se quebrarem os selos do ambiente protegido contra adulteração do SAM e/ou SCDev (ou sem que tal dê origem a um alarme de monitorização).

Do ponto de vista lógico, o ambiente protegido contra adulteração define vários tipos de utilizadores, com permissões diferentes e adequadas às suas funções, e com mecanismos de proteção adequados para garantir que o software só é usado para os fins pretendidos.

O ambiente protegido contra adulteração é operado dentro do ambiente protegido do SCMD (ver requisito na secção 6.2.13), não existindo qualquer ligação direta a partir da Internet, sendo ainda garantida a integridade do código executado neste ambiente.

6.2.13 Ambiente protegido do SCMD

O ambiente protegido do SCMD contém as várias componentes software e hardware constituintes do TW4S e é auditado de acordo com os requisitos para operação segura de um sistema de assinatura remoto. Dispõe dos mecanismos *state-of-the-art* para proteção de ataques da Internet (assim como proteção contra alterações não autorizadas de *software*, *hardware* e configurações) e é o intermediário nas ligações com os ambientes externos.

No que diz respeito ao ambiente externo de registo, a validação inicial do registo do cidadão para a emissão do certificado de assinatura qualificada remota CMD (processo de subscrição) é efetuada de acordo com o ETSI EN 319411-1, 6.2.2 e ETSI EN 319411-2, 6.2.2:

- O registo no SCMD pode ser presencial ou eletrónico, mas garantindo que o registo inicial foi efetuado presencialmente, ou seja, a validação inicial da identidade do requerente é sempre feita pelo método de "cara-a-cara", conforme descrito na secção 3.1;
- É verificada a identidade do cidadão, presencialmente nos locais de subscrição do serviço através da apresentação do Cartão de Cidadão, Passaporte ou Bilhete de Identidade, ou através do certificado de autenticação do Cartão de Cidadão aquando da subscrição via Internet. Em ambos os casos é verificada a autenticidade e validade do Cartão de Cidadão apresentado;
- Na verificação da identidade é obtido o nome completo, data de nascimento, NIC e validade do Cartão de Cidadão, a partir do Cartão de Cidadão – estes dados são utilizados para emissão do certificado de assinatura qualificada remota CMD e fazem parte do Distinguished Name (DN) do certificado. O número de telemóvel é fornecido pelo Cidadão, sendo validado/ativado através de OTP, e constitui um método de comunicação com o Cidadão.

No que diz respeito ao ambiente externo de emissão de certificado, o par de chaves é gerado pelo SCDev aquando do registo do cidadão no SCMD, sendo imediatamente enviado o correspondente *certificate request* à Entidade de Certificação. A chave privada gerada e correspondente chave pública são arquivados na *keystore* gerida pelo SCDev, cifrados com a palavra-chave introduzida pelo cidadão (ou com palavra-chave fornecida ao cidadão, no caso de registo presencial, que terá que alterar no *site* CMD antes da primeira utilização da chave privada), garantindo desse modo que o cidadão tem controlo sobre a chave privada associada à

chave pública enviada no *certificate request* à Entidade de Certificação, conforme requisito especificado em ETSI EN 319411-1, 6.3.1 a.

Note-se que as operações de geração do par de chaves, emissão do certificado qualificado CMD e guarda inicial do par de chaves constituem-se num processo atómico, na medida em que essas operações são sequenciais e, se alguma delas não for concretizada com êxito, as operações posteriores não são executadas e todas as anteriores são desfeitas.

6.2.14 Ambiente do assinante

O ambiente do assinante (titular do par de chaves utilizadas para a assinatura qualificada remota de um documento) é local ao assinante.

O cidadão é responsável pela proteção do seu ambiente local, a partir do qual efetua a assinatura qualificada remota de um documento.

6.2.15 Modelo funcional – Geral

As chaves privadas e o SAM estão protegidos por um ambiente protegido contra adulteração.

As chaves privadas só estão em claro no SCDev (HSM). O SAM encontra-se num ambiente protegido contra adulteração (cf. secção 6.2.12 e secção 6.2.50), dependendo do SCDev para toda a funcionalidade criptográfica e geração de números aleatórios.

6.2.16 Modelo funcional – Mecanismo de ativação de assinatura

A chave privada é gerada pelo SCDev, sendo cifrada pelo SCDev com a palavra-chave introduzida pelo cidadão, e guardada na *keystore* gerida pelo SCDev. Sempre que é necessária a sua utilização para assinar um documento submetido pelo titular da chave privada, a chave privada é decifrada e utilizada no SCDev sob o controlo exclusivo do seu titular, conforme descrição do protocolo SAP (cf. secção 3).

6.2.17 Modelo funcional – Mecanismo avançado de ativação de assinatura

O SSA comunica através de um canal seguro com o SAM, que verifica o SAD antes de ativar a chave de assinatura correspondente.

Um SAD está associado a um DTBS/R ou a um conjunto de DTBS/R dependendo se o utilizador está apenas a assinar um documento ou um conjunto de documentos.

A SIC é utilizada para criar uma ligação entre o assinante e a assinatura, através do SAD. A SIC recebe o SAD (código de segurança) gerado pelo SCDev a pedido do SAM, que é enviado pelo cidadão ao SAM, de forma segura, para validação.

6.2.18 Modelo funcional – Componentes TW4S

As componentes principais do TW4S são as seguintes componentes funcionais:

- Configuração da chave de assinatura – para gerar o par de chaves no SCDev e associá-la ao seu titular. Com base no pedido da Entidade de Registo, gera o par de chaves e o *certificate request* no SCDev, comunica com a Entidade de Certificação para obter o respetivo certificado digital e, guarda o par de chaves e certificado na *keystore* gerida pelo hardware criptográfico, cifrado com a palavra-chave de acesso à chave privada

introduzida pelo seu titular (ou com palavra-chave fornecida ao cidadão, no caso de registo presencial, que terá que alterar no *site* CMD antes da primeira utilização da chave privada);

- Gestão da chave de assinatura – Esta componente tem as funções de:
    - Inativação da chave de assinatura por pedido do seu titular,
    - Inativação da chave de assinatura por expiração da validade do certificado correspondente,
    - Alteração de palavra-chave de acesso à chave privada de assinatura;
- Autenticação do assinante – para autorizar a utilização da chave de assinatura pelo assinante. Esta ação é efetuada pelo SAM, de acordo com SAP;
- Criação de assinatura digital – para comunicar com o assinante autorizado, titular da chave de assinatura, de modo a criar a assinatura digital no SCDev. Esta componente é concretizada pela SSA, com quem a SCA comunica para criação/adição de assinatura a um documento, conforme identificado nos passos do SAP;
- SIC – para criar uma associação entre o assinante e a operação de assinatura, de acordo com o SAP. O SIC é (i) o telemóvel do cidadão, mais especificamente, o cartão SIM que recebe o SMS, e/ou (ii) a app executada no dispositivo (e.g., *tablet*, *smartphone*) do cidadão, que recebe a *Push notification* (conforme secção 6.2.10);
- SAM – protegido pelo ambiente protegido contra adulteração, é responsável pela operacionalização do SAP. Este módulo tem o seguinte conjunto de componentes funcionais:
    - Geração do SAD – para gerar o SAD no ambiente protegido contra adulteração. O código de segurança aleatório, que é enviado por SMS/*Push notification* para o SIC, é gerado no SCDev, a pedido do SAM;
    - Ativação da chave de assinatura – para gerir a validação do SAD e ativação da chave de assinatura, conforme SAP;
    - Geração da chave de assinatura – para gerir fatores de autenticação associados à chave de assinatura, conforme SAP.

6.2.19 Segurança – Gestão de sistemas e segurança

São definidas as seguintes funções no TW4S:

- Administradores de segurança, com as funções e responsabilidades indicadas para o Grupo de Trabalho de Administração de Segurança, na secção 5.2.1.3;
- Administradores de Sistemas, com as funções e responsabilidades indicadas para o Grupo de Trabalho de Administração de Sistemas, na secção 5.2.1.1;
- Operadores de Sistemas, com as funções e responsabilidades indicadas para o Grupo de Trabalho de Operação de Sistemas, na secção 5.2.1.2;
- Auditores de Sistemas, com as funções e responsabilidades indicadas para o Grupo de Trabalho de Auditoria de Sistemas, na secção 5.2.1.4.

6.2.20 Segurança – Gestão de operações

Os fornecedores das componentes TW4S fornecem as instruções de operação de modo a que as componentes TW4S sejam:

- Operadas de forma correta e segura;
- Implementadas de tal forma que o risco de falha nos sistemas seja minimizado;
- Protegidas contra vírus e software malicioso, para garantir a integridade dos sistemas e da informação que processam.

Os fornecedores das componentes TW4S fornecem documentação dos sistemas que cubram as responsabilidades das funções identificadas na secção 6.2.19, que deve incluir:

- Guia de Instalação;
- Guia de Administração;
- Guia do Utilizador.

6.2.21 Segurança – Sincronização de tempo

A criação de assinatura qualificada, a validação da expiração de um certificado e o registo de eventos auditáveis, são algumas das operações que têm uma relação e dependência direta do tempo, pelo que as várias componentes da TW4S têm que estar sincronizadas com uma fonte de tempo confiável.

Os vários sistemas do TW4S estão sincronizados com fontes de tempo confiável, garantindo rastreabilidade para o tempo UTC(k) através de um dos laboratórios UTC(k) identificados pelo BIPM (*Bureau International des Poids et Mesures*) na sua Circular T (https://www.bipm.org/en/bipm-services/timescales/time-ftp/Circular-T.html).

A sincronização é efetuada pelo protocolo NTP[12] em que o desvio máximo para o UTC[13] é de um segundo. Esta precisão é monitorizada, dando origem a um evento a investigar, sempre que for ultrapassada.

6.2.22 Segurança – Identificação e autenticação – Autenticação de utilizadores que não o assinante

A identificação e autenticação restringem o acesso e a utilização das componentes do TW4S às pessoas autorizadas, de tal forma que:

- Cada utilizador tem de se identificar e ser autenticado com sucesso antes que possa efetuar qualquer ação em nome do utilizador ou da função assumida pelo utilizador;
- Após *logout* é obrigatório efetuar nova autenticação;
- Se for utilizada combinação de dados de autenticação, a mesma será imprevisível;
- Existem mecanismos implementados que reduzem o risco de uma sessão autenticada ser assumida por outro utilizador, no caso do dispositivo de acesso ser deixado sem vigilância

[12] NTP – *Network Time Protocol*, de acordo com RFC 5905 (*Network Time Protocol Version 4: Protocol and Algorithms Specification*)

[13] UTC – *Coordinated Universal Time*

6.2.23 Segurança – Identificação e autenticação – Falha de autenticação

No TW4s, após a quinta tentativa de autenticação sem sucesso, a autenticação fica bloqueada – caso em que o cidadão tem que se deslocar ao balcão de registo e pedir ao operador para desbloquear o acesso –.

6.2.24 Segurança – Gestão de controlo de acesso a sistema

Os seguintes controlos são aplicados no acesso, pelo administrador de sistemas e/ou administrador de segurança, a todos os objetos sensíveis do TW4S:

- Limitar o acesso ao sistema ou objetos pelos quais são responsáveis, a indivíduos identificados;
- Controlar o acesso a informação sensível residual.

6.2.25 Segurança – Gestão de chaves – Geração de chave

O par de chaves é gerado e utilizado no SCDev, com credenciação CC EAL 4+ e/ou FIPS 140-2 *level* 3. O SCDev disponibiliza algoritmos criptográficos e tamanhos de chaves necessários para as necessidades de segurança identificadas.

O tamanho das chaves e algoritmos criptográficos suportados correspondem aos necessários para emitir par de chaves para assinatura qualificada, que utilizem os mesmos algoritmos e tamanho de chaves do par de chaves para assinatura qualificada incluídos no Cartão de Cidadão.

As chaves privadas de assinatura qualificada são guardadas na *keystore* gerida pelo SCDev, devidamente protegidas de modo a garantir a confidencialidade e integridade das mesmas.

O SCDev é inicializado em cerimónia auditada, em que estão presentes dois operadores (ou um administrador e um operador) do SCDev.

6.2.26 Segurança – Gestão de chaves – Armazenamento, *backup* e recuperação de chave

As chaves privadas de assinatura qualificada não são acedidas fora do SCDev, sendo guardadas numa *keystore* gerida pelo SCDev.

A guarda e recuperação das chaves privadas de assinatura qualificada é feito por meio de mecanismos automáticos, garantindo (através do SAP e SAM) que a chave é apenas utilizada pelo seu titular.

6.2.27 Segurança – Gestão de chaves – Utilização de chave

A chave privada é utilizada apenas para os fins previstos, i.e., para assinatura qualificada de documentos submetidos pelo titular da mesma.

A chave privada não é partilhada e existem controlos (através do SAP e SAM) para proteger o seu acesso e utilização.

A chave privada está apenas associada a um único assinante/titular e a um único certificado digital. Os processos de geração do par de chaves de assinatura qualificada garantem que só tem um titular e apenas é emitido um certificado para a mesma chave privada. A geração de cada par de chaves só é efetuada após pedido do cidadão (o cidadão só pode ter um par de chaves ativo,

para assinatura qualificada remota), sendo o par de chaves descartado/apagado se existir algum erro nas operações de geração de *certificate request*, pedido de certificado e guarda da chave privada e certificado na *keystore*, tal como referido na secção 6.1.

6.2.28 Segurança – Gestão de chaves – Distribuição de chave

A chave privada de assinatura não é entregue ao titular da mesma, ficando o par de chaves guardado em keystore gerida pelo SCDev.

6.2.29 Segurança – Gestão de chaves – Renovação / atualização / alteração de chave

Os algoritmos e tamanhos das chaves são analisados anualmente, sendo alterados no caso de se terem tornado inadequados.

Caso alguma chave privada tenha sido comprometida (ou existem suspeitas de estar comprometida), o certificado digital correspondente é imediatamente revogado e a chave privada é apagada do SCDev.

6.2.30 Segurança – Gestão de chaves – Arquivo de chave

Não é efetuado arquivo das chaves privadas de assinatura qualificada.

6.2.31 Segurança – Gestão de chaves – Eliminação de chave

A chave privada de assinatura qualificada é eliminada após a revogação ou expiração da validade do certificado digital correspondente.

6.2.32 Segurança – Auditoria – Geração de dados de auditoria

São gerados os seguintes eventos de auditoria:

- Gestão de chaves (geração, utilização e eliminação);
- Eventos de assinatura de documentos;
- Autenticação do utilizador titular do par de chaves durante o SAP;
- Gestão do SAD do assinante (i.e., titular do par de chaves) – geração, envio e validação do SAD;
- Início e fim da função de geração de dados de auditoria;
- Alteração aos parâmetros de auditoria;
- Tentativas de acesso às várias componentes do TW4S.

6.2.33 Segurança – Auditoria – Garantia de disponibilidade dos dados de auditoria

Os logs de auditoria são arquivados (conforme secção 6.2.40) durante o tempo estabelecido por lei. No caso dos logs de registo das assinaturas eletrónicas qualificadas efetuadas, estes são

arquivados até um ano após a revogação ou cancelamento do respetivo certificado qualificado CMD.

Os logs de auditoria estão protegidos contra eliminação não autorizada.

6.2.34 Segurança – Auditoria – Parâmetros dos dados de auditoria

Cada registo de evento de auditoria contém os seguintes parâmetros:

- Data e hora do evento;
- Tipo de evento;
- Identidade da entidade responsável pela ação;
- Sucesso ou falha do evento.

6.2.35 Segurança – Auditoria – Pesquisa de eventos de auditoria

Os registos de eventos de auditoria podem ser pesquisados por qualquer parâmetro, assim como podem ser processados e apresentados de forma a serem interpretados por elemento(s) do Grupo de Trabalho de Auditoria de Sistemas.

6.2.36 Segurança – Auditoria – Restrição na auditoria

O SCMD nega o acesso de todos os utilizadores aos registos de eventos de auditoria, à exceção dos utilizadores a que seja explicitamente autorizado o acesso de leitura.

6.2.37 Segurança – Auditoria – Geração de avisos

O SCMD dispõe de um sistema de monitorização *state-of-the-art*, em que eventos inusuais, incomuns ou bem tipificados, que podem ter impacto na capacidade de operação ou na segurança do TW4S, dão origem a uma notificação de evento a investigar pelos administradores de sistemas ou, desencadeiam ações automáticas para reagir a possíveis ataques.

6.2.38 Segurança – Auditoria – Garantia de integridade dos dados de auditoria

O SCMD garante a integridade dos registos de eventos de auditoria. Disponibiliza ainda uma aplicação para verificar a integridade dos registos de eventos de auditoria, utilizada pelo sistema de monitorização e pelo(s) elemento(s) do Grupo de Trabalho de Auditoria de Sistemas.

6.2.39 Segurança – Auditoria – Data/hora dos dados de auditoria

Como referido na secção 6.2.21, os vários sistemas do TW4S estão sincronizados por NTP, pelo que o parâmetro data e hora de cada registo de evento de auditoria beneficia desse sincronismo.

6.2.40 Segurança – Arquivo – Geração de dados de arquivo

O SCMD gera um arquivo de registos de eventos de auditoria em media externo, apropriado para armazenamento e processamento desses arquivos (durante o tempo indicado na secção 6.2.33), e fornecendo as evidências legais necessárias para sustentar a correção das assinaturas digitais qualificadas. O arquivo não inclui parâmetros sensíveis de segurança (que também não são incluídos nos registos de eventos de auditoria).

Cada arquivo inclui a data e hora a que ocorreu, de acordo com os requisitos da secção 6.2.39.

6.2.41 Segurança – Arquivo – Integridade dos arquivos

A modificação não autorizada dos arquivos é prevenida, através da eliminação da permissão de escrita de todos os arquivos. Adicionalmente um mecanismo automático verifica a integridade dos arquivos e caso seja verificada alguma modificação, lança um evento de monitorização que será investigado.

6.2.42 Segurança – Backup e recuperação – Integridade e confidencialidade dos backups

São efetuados backups dos sistemas do SCMD (à exceção do SCDev) e de todos os dados necessários para recuperar o SCMD após uma falha ou desastre.

Os backups são protegidos contra modificações por mecanismo que permite verificar a integridade dos mesmos. Os parâmetros sensíveis de segurança e outra informação confidencial é guardada de forma protegida, de forma a garantir a integridade e confidencialidade da mesma.

6.2.43 Segurança – Backup e recuperação – Recuperação

O SCMD inclui funções de recuperação que permitem restaurar o estado a partir de um backup. O operador de Sistemas pode invocar a função de recuperação, em caso de necessidade.

6.2.44 Segurança das componentes principais – Configuração da chave de assinatura – Chave criptográfica

Os algoritmos e tamanho de chaves utilizados para o par de chaves de assinatura qualificada foram escolhidos de modo a que possam resistir durante o tempo de vida do certificado associado à chave privada e, tal como referido na secção 6.2.25, são os mesmos do par de chaves para assinatura qualificada incluídos no Cartão de Cidadão.

O par de chaves de assinatura qualificada de um assinante está associado ao devido certificado do assinante/titular, de acordo com o processo de geração do par de chaves (cf. secção 6.2.27) e o processo de subscrição (cf. secção 6.2.13).

A chave privada não pode ser usada antes do certificado correspondente estar associado no TW4S, decorrendo tal do processo de subscrição (cf. secção 6.2.13) que garante também a integridade da ligação entre a chave privada e o certificado digital correspondente.

6.2.45 Segurança das componentes principais – Autenticação do assinante

A subscrição do serviço e validação inicial do cidadão (assinante/titular do par de chaves) está descrita na secção 6.2.13 e garantem que:

- A subscrição/*enrolment* está conforme a *assurance level high* nas componentes "*Application and registration*" e "*Identity proofing and verification (natural person)*" da (EU) 2015/1502[14] Clause 2.1;
- As características do meio eletrónico de identificação estão conforme a *assurance level high* na componente "*Electronic identification means characteristics and design*" – (EU) 2015/1502[14] Clause 2.2.1;
- O mecanismo de autenticação está conforme a *assurance level high* da (EU) 2015/1502[14] Clause 2.3.1.

Os controlos implementados, os passos do SAP e o SAM garantem o seguinte:

- A SSA requer que o assinante tenha sido identificado e autenticado antes de permitir qualquer ação que possa afetar o controlo exclusivo da chave de assinatura;
- Os protocolos em utilização previnem os ataques de repetição e de *man-in-the-middle*, assim como outras formas de ataque em que um utilizador malicioso possa utilizar credenciais que não lhe pertencem;
- Os controlos de acesso garantem que um assinante não tem acesso a componentes sensíveis ou funções do sistema que lhe permitam controlar a chave de assinatura de outro assinante;
- O DTBS/R fornecido pelo assinante é assinado apenas pela chave de assinatura de que esse assinante é titular.

6.2.46 Segurança das componentes principais – Autenticação do assinante – Gestão de falhas de autenticação

O SCMD deteta a ocorrência de falhas consecutivas de autenticação de um assinante (titular do par de chaves), conforme secção 6.2.23

6.2.47 Segurança das componentes principais – Autenticação do assinante – Autenticação do assinante delegada a sistema externo

Não aplicável.

6.2.48 Segurança das componentes principais – Criação da assinatura – Operação criptográfica

O algoritmo de assinatura utilizado é o sha256WithRSAEncryption.

[14] *Commission Implementing Decision (EU) 2015/1502 of 8 September 2015, on setting out minimum technical specifications and procedures for assurance levels for electronic identification means*.

6.2.49 Segurança adicional – Geral

Os passos do SAP e o SAM garantem o seguinte:

- O assinante é autenticado direta ou indiretamente pelo SAM;
- O SAD é obtido, com um alto grau de confiança, sob o controlo único do assinante, garantindo que a chave de assinatura é utilizada pelo assinante autenticado para um DTBS/R específico.

6.2.50 Segurança adicional – SAP e SAD – Resistência a ameaças

A subscrição do serviço e validação inicial do cidadão (assinante/titular do par de chaves) está descrita na secção 6.2.13 e garantem que:

- A subscrição/*enrolment* está conforme a *assurance level high* nas componentes "*Application and registration*" e "*Identity proofing and verification (natural person)*" da (EU) 2015/1502[14] Clause 2.1;
- As características do meio eletrónico de identificação estão conforme a *assurance level high* na componente "*Electronic identification means characteristics and design*" – (EU) 2015/1502[14] Clause 2.2.1;
- O mecanismo de autenticação está conforme a *assurance level high* da (EU) 2015/1502[14] Clause 2.3.1.

O passos do SAP e o SAM, assim como os protocolos utilizados para estabelecer as várias ligações e os controlos implementados garantem o seguinte:

- Os controlos implementados contrariam as seguinte ameaças sobre o SAD e sobre a utilização do SAD: *online guessing, offline guessing, credential duplication, phishing, eavesdropping, replay, session hijacking, man-in-the middle, credential theft, spoofing and masquerading attacks*;
- O SAP disponibiliza mecanismos criptográficos fortes que protegem os fatores de autenticação contra ameaças ao protocolo utilizado assim como contra ataques de personificação de terceiras partes de confiança;
- O SAD está protegido contra ataques de repetição, falsificação e *bypass* entre o assinante e o SCDev remoto;
- O SAP foi desenhado de modo a poder ser assumido que o SAD está protegido de forma segura contra ataques de duplicação ou adulteração efetuados por um atacante com alto potencial de ataque;
- O SAP foi desenhado de modo que o assinante possa proteger, de forma segura, a ativação da chave de assinatura pelo SAD, contra um atacante com alto potencial de ataque.

O SAM é utilizado num ambiente protegido contra adulteração (cf. secção 6.2.12), dependendo do SCDev (com credenciação FIPS 140-2 nível 3 e/ou *Common Criteria* EAL 4+) para toda a funcionalidade criptográfica e geração de números aleatórios.

6.2.51 Segurança adicional – SAP e SAD – Gestão

O SAD é constituído pelo código de segurança, gerado pelo SCDev a pedido do SAM e, enviado pelo SAM para o SIC do cidadão/signer, sendo introduzido pelo cidadão no *user interface* da SCA.

O SAP, SAD e SAM garantem o seguinte:

- O SAD é enviado para o SIC, que se encontra sob o controlo único do assinante, com um alto grau de confiança;
- O SAD é o resultado de uma operação criptográfica que associa com um alto grau de confiança o DTBS/R com os dados de identificação do assinante autenticado e, com a chave de assinatura do assinante;
- O SAD só ativa a chave de assinatura no caso da autenticação do assinante ter sido efetuada com sucesso. Nessa medida, o SAD só é gerado e enviado ao assinante, após a sua autenticação com sucesso no SCMD;
- O SAP é desenhado de tal modo que quando o SAD é recebido pelo SAM, pode ser assumido que o SAD foi submetido sob o controlo único do assinante, através de meios que estão na posse do assinante;
- O SAD é verificado de tal forma que é altamente improvável que atividades como adivinhar, espiar, repetir ou manipular a comunicação por um atacante com alto potencial de ataque possa subverter a autenticação para a ativação da assinatura.

6.2.52 Segurança adicional – Gestão da chave de assinatura – Geração da chave de assinatura

O par de chaves é gerada e utilizada num SCDev que cumpre os requisitos FIPS 140-2 nível 3 e/ou *Common Criteria* EAL 4+. O SCDev é utilizado para suportar todas as funções criptográficas necessárias para o serviço de criação de assinaturas qualificadas, disponibilizado pelo SCMD.

O SCDev gera e gere o par de chaves dos diferentes assinantes, sendo que apenas existe um par de chaves de assinatura por cada assinante.

O desenho do SAP garante uma alta confiança na ligação entre a chave de assinatura e o ser titular/assinante.

A chave privada não pode ser usada antes do certificado correspondente estar associado no TW4S, decorrendo tal do processo de subscrição (cf. secção 6.2.13) que garante também a integridade da ligação entre a chave privada, o certificado digital correspondente e o seu titular/assinante.

6.2.53 Segurança adicional – Gestão da chave de assinatura – Ativação da chave de assinatura

O SAP e SAM garantem o seguinte:

- O assinante tem que fornecer a SAD ao SAM, de modo a ser autenticado e ativar a chave de assinatura;
- O SAP gere a transmissão do SAD ao SAM de tal modo que garante que a chave de assinatura está sob controlo do assinante (titular da chave de assinatura), com um alto grau de confiança;
- A chave de assinatura do assinante será ativada apenas para utilização num SCDev remoto;
- A chave de assinatura do assinante é ativada pelo SAD gerado para o assinante;
- A chave de assinatura ativada é usada apenas para assinar o DTBS/R autorizado pelo SAP;

- Após a ativação da chave de assinatura e a criação da assinatura digital, o SAD do assinante é apagado.

Os utilizadores dos sistemas TW4S não têm privilégios para utilizarem a chave privada de um assinante.

7 Auditoria de conformidade e outras avaliações

As auditorias de conformidade e outras avaliações efetuadas pela EC CMD estão descritos na DPC da EC CMD.

Nesta secção descrevem-se as auditorias de conformidade e outras avaliações efetuadas pela TW4S e pela Entidade de geração e guarda de par de chaves.

Uma das funções do Grupo de Trabalho de Auditoria de Sistemas é efetuar auditoria interna a todas as ações relevante e necessárias para assegurar a operacionalidade do SCMD, entre as quais se enquadra a auditoria de que o SCMD está conforme esta DPO e Políticas associadas. Para além da auditoria interna, todas as cerimónias serão acompanhadas e auditadas pelo Grupo de Trabalho de Auditoria de Sistemas.

Outras auditorias e avaliações serão englobadas nas auditorias efetuadas pela AMA aos seus sistemas e redes informáticas, podendo também ser requeridas pelo Grupo de Trabalho de Gestão. Estas auditoria e avaliações poderão ser executadas por entidades externas.

O auditor interno, nomeado pela Direção da AMA, é membro por inerência do Grupo de Trabalho de Auditoria de Sistemas do SCMD, mantendo a sua independência em relação aos restantes Grupos de Trabalho do SCMD. Em termos de qualificações, o auditor interno deve preencher os requisitos indicados na secção 5.2.1.4. Os auditores e avaliadores externos são pessoas ou organizações de reconhecida idoneidade, independentes da AMA e dos fornecedores de produtos e soluções do SCMD, com experiência e qualificações comprovadas na área em que efetuem a auditoria ou avaliação.

No final da auditoria (ou avaliação), o auditor (interno ou externo):

- Até 24 horas após a auditoria:
    a) Elabora um relatório resumido de primeiras impressões (RRPI), em que indica as não conformidades encontradas durante a auditoria e o seu grau de gravidade;
    b) Reúne com os elementos do Grupo de Trabalho de Administração de Segurança e apresenta o RRPI;
- Até 1 semana após a auditoria:
    a) Elabora o relatório final da auditoria (RFA) e remete uma cópia ao Grupo de Trabalho de Administração de Segurança. Este relatório é organizado de modo a que as não conformidades estejam escalonadas por ordem decrescente de gravidade.

Após a receção do RRPI e/ou RFA, o Grupo de Trabalho de Administração de Segurança segue o seguinte procedimento:

1. Avalia o relatório;
2. Caso existam não conformidades,
    a. Convoca os elementos dos Grupos de Trabalho que considerar conveniente, para validar e analisar as situações reportadas;
    b. Propõe as medidas adequadas ao Grupo de Gestão, de acordo com esta DPO e Políticas. Estas medidas podem incluir, entre outras, suspensão ou continuação temporária das operações até estarem resolvidas as não conformidades, revogação de certificados emitidos, mudança nos membros

dos Grupos de Trabalho, pedidos de indemnização, processos jurídicos e auditorias adicionais;

c. Após decisão do Grupo de Gestão, acompanha a implementação das medidas corretivas, ou outras;

d. Arquiva toda a informação recolhida assim como as ações tomadas, de acordo com secção 5.5;

3. Dá conhecimento aos Grupos de Trabalho e arquiva o relatório, conforme secção 5.5.

Os relatórios de auditorias, avaliações e ações subsequentes são de acesso restrito aos elementos do Grupo de Trabalho de Administração de Segurança, Grupo de Gestão e, Administração da AMA.

7.1 Auditoria de conformidade

A auditoria de conformidade é realizada de acordo com o regulamento 910/2014 e do despacho 155/2017 (Criação de assinaturas eletrónicas à distância, com gestão por um prestador qualificado de serviços de confiança em nome do signatário), de 5 de Dezembro de 2017, do Gabinete Nacional de Segurança (GNS);

8 Outros assuntos comerciais e legais

Esta secção abrange assuntos jurídicos e outros negócios em geral, no âmbito da TW4S e da Entidade de geração e guarda de par de chaves.

8.1 Modelo de sustentabilidade

O modelo de sustentabilidade segue o artigo 11º da Portaria_CMD.

8.2 Responsabilidade financeira

O SCMD disponibiliza ferramentas tecnológicas que permitem criar uma assinatura "server-side" sob o controlo exclusivo do titular da chave de assinatura (e respetivo certificado), não fazendo qualquer análise sobre o documento fornecido para assinar, sendo a assinatura da inteira responsabilidade do seu titular.

8.3 Confidencialidade da informação de negócio

Toda a informação disponibilizada no repositório (cf. secção 2) é considerada informação não confidencial ou pública, sendo acessível publicamente.

Toda a restante informação do SCMD é considerada confidencial, tendo acesso restrito.

Entidades (pessoas ou empresas) autorizadas que recebam informação confidencial são responsáveis por assegurar que esta não é copiada, reproduzida, armazenada ou transmitida a terceiras partes, por quaisquer meios, sem antes terem o consentimento escrito da AMA.

8.4 Privacidade de dados pessoais

Aplicam-se as disposições estabelecidas no artigo 12º (Segurança de dados) da Portaria CMD.

8.5 Propriedade Intelectual

Todos os direitos de propriedade intelectual referentes ao SCMD pertencem à AMA.

8.6 Garantias

O SCMD fornece as seguintes garantias:

- Realiza as suas operações de acordo com esta DPO e Políticas indicada na secção 1.1;
- Utiliza sistemas e produtos fiáveis que estejam protegidos contra toda a alteração e que garantam a segurança técnica e criptográfica dos processos de geração e guarda de par de chaves e, assinatura "*server-side*";
- Os membros dos Grupos de Trabalho exercem as funções e têm as qualificações identificadas na secção 5.2.1;
- Opera o repositório que disponibiliza publicamente toda a informação identificada na secção 2;

- Não utiliza certificado digital emitida pela EC CMD que não esteja válido, quer por ter sido revogado ou ter sido ultrapassado o seu prazo de validade;
- Revoga os certificados emitidos pela EC CMD quando acaba o seu período de validade, apagando a respetiva chave privada;
- Opera de acordo com a legislação aplicável;
- Colabora com as entidades judiciais e outras entidades que tenham poderes de supervisão sobre a AMA.

As terceiras partes confiantes nas assinaturas "server-side" criadas pelo SCMD têm por obrigação:

- Comprovar que o certificado associado à chave privada utilizada na assinatura "*server-side*" se encontra dentro do seu período de validade e consultar a respetiva LCR ou serviço OCSP (preferencialmente) para verificar que não está revogado;
- Verificar que o certificado pertence ao autor do documento assinado e, foi emitido na hierarquia da EC CMD;
- Assumir a responsabilidade na correta verificação das assinaturas digitais;
- Conhecer e aceitar a DPO e Políticas associadas à assinatura em que confia.

O subscritor do serviço SCMD tem por obrigação:

- Tomar todos os cuidados e medidas necessárias para garantir a segurança da palavra-chave de acesso à sua chave de assinatura;
- Não fornecer a terceiros o código de segurança para ativação de assinatura, recebido por mensagem SMS (ou por *Push notification*) no seu telemóvel ou *app*/dispositivo;
- Validar que os dados de identificação do documento a assinar, recebidos na mensagem SMS/*Push notification*, são os mesmos que lhe são apresentados no *user interface* do SCA, e que o NIC é o seu;
- Abster-se de assinar documentos de que não é autor ou para os quais não tem a devida autorização;
- De-subscrever o serviço SCMD sempre que o seu telemóvel/dispositivo associado ao SCMD for perdido, roubado, alterado ou inutilizado;
- De-subscrever o serviço SCMD sempre que alterar o seu número de telemóvel associado ao SCMD;
- Não monitorizar, manipular ou efetuar ações de "engenharia inversa" sobre a implantação técnica dos serviços SCMD, sem a devida autorização prévia, por escrito, da AMA.

8.7 Isenção de Garantias

O SCMD não se vincula a qualquer garantia que não esteja estabelecida nesta DPO e Políticas anexas ou relacionadas.

8.8 Limitação de Responsabilidade

– A AMA assume a responsabilidade perante terceiros pela atuação dos titulares das funções necessárias à prestação de serviços SCMD.

- A responsabilidade da administração / gestão do SCMD assenta sobre base objetiva e cobre todo o risco que os particulares sofram sempre que seja consequência do funcionamento normal ou anormal dos seus serviços.
- A AMA não responde se o destinatário dos documentos assinados eletronicamente não os comprovar e tiver em conta as restrições que figuram no certificado quanto às suas possíveis utilizações.
- A AMA não assume qualquer responsabilidade no caso de perca ou prejuízo:
    - Dos serviços que prestam, em caso de guerra, desastres naturais ou qualquer outro caso de força maior;
    - Ocasionados pelo uso indevido ou fraudulento dos certificados utilizados na assinatura "*server-side*".

8.9 Indemnização

De acordo com a legislação em vigor.

8.10 Prazo e rescisão

Esta Declaração de Práticas de Operação e Política anexas ou relacionadas:

- entra em vigor no momento da sua aprovação pelo Grupo de Trabalho de Gestão e publicação no repositório (cf. secção 2);
- termina o seu efeito quando ocorrer o fim da atividade do SCMD, após serem efetuados os passos referentes ao fim de atividade conforme secção 5.7 desta DPO.

Durante o período em que estão em vigor, a DPO e Políticas anexas ou relacionadas podem ser substituídas, conforme descrito na secção 8.12.

8.11 Avisos individuais e comunicação com os participantes

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

8.12 Alterações

Durante o período em que estão em vigor, a DPO e Política anexas ou relacionadas podem ser alteradas e substituídas.

Sempre que algum destes documentos for substituído, essa informação será publicada no *site web* SCMD.

8.12.1 Versões

As alterações à DPO e Política anexas ou relacionadas são propostas pelo Grupo de Trabalho de Administração de Segurança e são aprovadas pelo Grupo de Trabalho de Gestão, antes da nova versão ser publicada no repositório SCMD. A nova versão do documento torna-se efetiva e entra em vigor imediatamente após a sua publicação, independentemente das mudanças efetuadas no mesmo, substituindo de forma integral todas as versões anteriores do documento.

A versão do documento tem o formato N.X, sendo N e X inteiros e, correspondendo

- N à versão pública do documento, incrementado de um (1) a cada nova versão,
- X à versão interna de alterações e para cada versão pública do documento, o valor de X é inicializado a zero (0).

A primeira versão de cada documento publicado é a versão 1.0.

8.13 Resolução de litígios

Todas as reclamações dos participantes no SCMD, definidos na secção 1.3, devem ser comunicados ao Grupo de Trabalho de Gestão que tentará resolvê-las.

Para a resolução de qualquer litígio que possa surgir com relação a esta DPO e Política anexas ou relacionadas, as partes, com renúncia a qualquer outro foro, submetem-se à Jurisdição de Contencioso Administrativo.

8.14 Legislação aplicável

É aplicável à atividade do SCMD a legislação portuguesa e europeia, nomeadamente a legislação e as obrigações regulamentares e contratuais que contribuem para a operação e disponibilização do SCMD, que incluem:

- Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014 relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno;
- Despacho 155/2017 (Criação de assinaturas eletrónicas à distância, com gestão por um prestador qualificado de serviços de confiança em nome do signatário), de 5 de Dezembro de 2017, do Gabinete Nacional de Segurança;
- Decreto-Lei nº 290-D/99, de 2 de Agosto, em todos os pontos que não forem contrariados pelo Regulamento (UE) n.º 910/2014;
- Lei n.º 37/2014, de 26 de Junho com as alterações introduzidas pela Lei n.º 32/2017, de 1 de Junho, e respetiva regulamentação;
- Lei nº 67/98, de 26 de Outubro (Lei da proteção de dados pessoais);
- Decreto-Lei nº 36/2003 (Código da propriedade industrial);
- Lei nº 41/2004 (Lei da proteção de dados pessoais no sector das comunicações eletrónicas);
- Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados);

- Regulamento (UE) nº 611/2013 do Parlamento Europeu e do Conselho, de 24 de Junho de 2013, relativo às medidas aplicáveis à notificação e violação de dados pessoais;
- Lei das Comunicações Eletrónicas, aprovada pela Lei nº 5/2004 de 10 de Fevereiro;
- Decisão da Autoridade Nacional de Comunicações (ANACOM), aprovada por deliberação do respetivo Conselho de Administração, de 12 de Dezembro de 2013, relativa às exigências de comunicação e divulgação ao público de violações de segurança ou perdas de integridade ocorridas em redes e serviços de comunicações;
- Lei nº 109/2009, de 15 de Setembro (Lei do Cibercrime);
- Regulamento (CE) nº 593/2008 do Parlamento Europeu e do Conselho, de 17 de Junho de 2008, sobre a lei aplicável às obrigações contratuais (Roma I);
- Regulamento (CE) nº 864/2007 do Parlamento Europeu e do Conselho, de 11 de Julho de 2007, relativo à lei aplicável às obrigações extracontratuais (Roma II).

8.15 Conformidade com a legislação em vigor

Esta DPC e PCs correspondentes estão em conformidade com a legislação identificada na secção 8.14. Adicionalmente está em conformidade com a legislação nacional e europeia relativa à limitação de importação e exportação de *software* e *hardware* criptográfico.

8.16 Finalização ou alteração de prestação do serviço de confiança SCMD

A atividade do SCMD será suspensa, alterada ou terminada em caso de ato administrativo ou legislativo que o imponha.

Em qualquer um dos casos, a entidade supervisora (GNS) e os subscritores do SCMD serão informados adequadamente.

Após a finalização da atividade do SCMD, e no mais curto espaço de tempo tecnicamente possível, serão revogados todos os certificados dos subscritores ainda ativos. Os dados sujeitos a arquivo continuarão arquivados pelo período de tempo definido pela legislação nacional e/ou regulamento 910/2014, ficando à guarda da entidade identificada no ato administrativo ou legislativo de finalização da atividade do SCMD – caso nenhuma entidade seja identificada, os dados serão entregues à entidade supervisora.

8.17 Disposições diversas

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

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

Aprovação

Aprovado pelo Grupo de Trabalho de Gestão.

Assinado por : **ANDRÉ FERREIRA FERRÃO COUTO E VASCONCELOS**
Num. de Identificação: BI111164753
Data: 2019.05.13 09:19:21 GMT Daylight Time

Assinado por : **RITA SUZINDA LOURENÇO PINTO REI**
Num. de Identificação: BI102699577
Data: 2019.05.13 12:48:56 Hora de Verão de GMT