AUTENTICAÇÃO.GOV
CHAVE MÓVEL DIGITAL

Política CMD de assinatura qualificada

Políticas (POL#16)

Nível de Acesso: Público

Versão: 2.0

Data: 19/Mar/2018

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, Assinatura Qualificada

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	19/Mar/2018	Adição de número de portaria CMD.

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 Operação	AMA	Descreve os procedimentos e práticas utilizados pelo SCMD para suportar a sua atividade de assinatura eletrónica qualificada "*server-side*".

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

1.1 Visão Geral

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*" (ou, assinatura eletrónica qualificada à distância) 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.

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.

A política CMD 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 indicado em:

- "Declaração de Práticas de Operação", que descreve os procedimentos e práticas utilizados pelo SCMD para suportar a sua atividade de assinatura eletrónica qualificada "server-side";
- "Condições gerais de utilização do serviço SCMD", que descreve as condições de utilização do serviço SCMD, para aceitação pelo titular do certificado CMD de assinatura qualificada e utilizador do serviço SCMD.

1.2 Domínio de aplicação

1.2.1 Âmbito e limites da política de assinatura

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 (cf. secção 1.2.2).

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.

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.

1.2.2 Aplicações

As aplicações[1] disponibilizadas/autorizadas pela AMA que permitem que os assinantes efetuem a criação de assinaturas qualificadas através do SCMD, de acordo com a política CMD de assinatura qualificada, estão elencadas no sítio do SCMD, em https://www.autenticacao.gov.pt/cmd-assinatura. À data de publicação deste documento, estavam indicadas as seguintes aplicações:

i. Aplicação Oficial do Cartão de Cidadão Português
    - Versão: 3.0 ou superior;
    - Fornecedor da aplicação: 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;
    - Tipo de documento a assinar: PDF;
    - Disponível em: https://www.autenticacao.gov.pt/cc-software;
    - Sistema operativo: Windows, MacOS e Linux;
    - Contexto transacional: Assinatura de documento em formato PDF submetido pelo cidadão, titular do par de chaves e certificado CMD. O fornecedor da aplicação não analisa o documento fornecido para assinar, pelo que a aposição da assinatura não presume concordância com o seu conteúdo.

1.2.3 Contexto transacional

O contexto transacional é indicado para cada aplicação na secção 1.2.2.

[1] Estas aplicações são também designadas por SCA (*Signature Creation Application*).

1.3 Nomes de documentos e políticas, identificação e regras de conformidade

1.3.1 Documento de política de assinatura e nomes da(s) política(s) de assinatura

Este documento é o documento de política de assinatura com o nome de "Política CMD de assinatura qualificada" e, define uma única política (um único conjunto de regras) com o mesmo nome do documento.

1.3.2 Documento de política de assinatura e identificador(es) da(s) política(s) de assinatura

Este documento é identificado pelo número único – designado de "identificador de objecto" (OID[2]) – 2.16.620.2.1.2.2, que também identifica a política.

Identificação do Documento	
Nome	Política CMD de assinatura qualificada
OID	2.16.620.2.1.2.2
Versão	2.0

1.3.3 Regras de conformidade

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).

1.3.4 Pontos de distribuição

Este documento está disponível em versão PDF no repositório do SCMD, indicado na secção 2 (Repositório e Publicação) da "Declaração de Práticas de Operação".

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

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

1.4 Administração do documento de Política de assinatura

1.4.1 Autoridade da Política de assinatura

A entidade responsável e com autoridade sobre o presente documento de política de assinatura é a AMA – Agência para a Modernização Administrativa, I.P..

Nome:	AMA – Agência para a Modernização Administrativa, I.P.
Morada:	Rua Abranches Ferrão n.º 10, 3º G 1600-001, Lisboa Portugal
NIF:	508 184 509
Registo:	Registada na Conservatória do Registo Comercial de Lisboa com o número: 508184509
Correio Eletrónico:	ama@ama.pt
Telefone:	+351 217 231 200

O presente documento de política de assinatura está assinado digitalmente por pelo menos dois elementos do Grupo de Trabalho de Gestão, através de certificado qualificado.

1.4.2 Contacto

Todos os contactos referentes ao documento de Política de assinatura devem ser direcionados para a autoridade da política de assinatura (cf. secção 1.4.1), ao cuidado do Grupo de Trabalho de Administração de Segurança do SCMD.

1.4.3 Procedimentos de aprovação

O Grupo de Trabalho de Administração de Segurança (GTAS) determina a conformidade e aplicação da Política (e Declaração de Práticas de Operação). 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 para revisão e aprovação. Após a aprovação, as novas versões dos documentos são disponibilizadas publicamente, substituindo a versão anterior.

1.5 Definições e Acrónimos

As definições e acrónimos gerais do SCMD devem ser consultadas na secção respetiva da Declaração de Práticas de Operação. Esta secção contém as definições e acrónimos específicos a este documento.

Termo	Descrição
Aplicação de criação de assinatura	Aplicação no âmbito do sistema de criação de assinatura que cria a assinatura digital, excluindo o dispositivo de criação de assinatura (conforme ETSI EN 319 102-1). No caso do SCMD, a aplicação de criação de assinatura é a SSA (conforme definida na "Declaração de Práticas de Operação").
Aplicação de validação de assinatura	Aplicação que implementa o processo de verificar e confirmar que uma assinatura é válida.
Aumento da assinatura	Processo de incorporação de informação na assinatura digital, com o objetivo de manter a validade dessa assinatura a longo prazo. Aumentar as assinaturas é um processo colateral para a posterior validação de assinaturas, ou seja, o processo pelo qual determinada informação (por exemplo, selo de tempo, dados de validação e até mesmo dados relacionados com o arquivo) é incorporada nas assinaturas para torná-las mais resistentes a alterações ou para ampliar a sua longevidade.
Dispositivo de criação de assinatura	Software ou hardware configurado, que utilizam chaves e mecanismos criptográficos para criarem uma assinatura digital.
Driving application	Aplicação que utiliza uma aplicação/sistema de criação de assinatura para criar uma assinatura, ou que utiliza uma aplicação de validação de assinatura para validar assinaturas digitais (conforme ETSI EN 319 102-1). No caso do SCMD, a *driving application* é a SCA (conforme definida na "Declaração de Práticas de Operação").
Política de assinatura	Política de criação de assinatura, política de aumento de assinatura, política de validação de assinatura, ou qualquer combinação destas políticas, aplicável à mesma assinatura ou conjunto de assinaturas.
Política de aumento de assinatura	Conjunto de regras, aplicável a uma ou mais assinaturas digitais, que definem os requisitos técnicos e processuais para o seu aumento, de modo a cumprir com uma necessidade particular de negócio. Abrange a coleta de informações e a criação de novas estruturas que permitam, a longo prazo, validar uma assinatura.
Política de criação de assinatura	Conjunto de regras, aplicável a uma ou mais assinaturas digitais, que definem os requisitos técnicos e processuais para a sua criação, de modo a cumprir com uma necessidade particular de negócio.
Política de validação de assinatura	Conjunto de regras, aplicável a uma ou mais assinaturas digitais, que definem os requisitos técnicos e processuais para a sua validação, de modo a cumprir com uma necessidade particular de negócio.
Validação de assinatura	Processo de verificação e confirmação da validade da assinatura digital.

2 Declarações de práticas de aplicação de assinatura

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:

- 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.

A política e os requisitos de práticas de segurança seguidos pelo SCMD na criação de assinatura estão em conformidade com:

- O contexto e requisito legal definido pelo 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;
- As regras para criação de uma assinatura qualificada eletrónica, como definido na legislação europeia, nomeadamente no regulamento 910/2014 (eIDAS);
- Os requisitos específicos definidos no Despacho 155/2017 do GNS;
- Os blocos de construção da política de assinatura, como definido no standard ETSI TS 119 172-1 v1.1.1 *Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents*.

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).

3 Parâmetros no âmbito de negócio (PAN)

3.1 PAN relacionados com o processo de negócio/aplicação

3.1.1 PAN (a): *Workflow* (sequência e *timing*) das assinaturas

O SCMD cria a assinatura digital qualificada, sob o controlo do titular da chave de assinatura, a partir da representação dos dados a serem assinados (DTBS/R) enviados por uma aplicação disponibilizada/autorizada pela AMA (cf. secção 1.2.2).

No processo de negócio do SCMD apenas é criada uma assinatura por cada DTBS/R recebido, pelo que não existe sequência de assinaturas a criar para um mesmo DTBS/R.

Embora o SCMD registe a hora exata em que a assinatura é criada, não aumenta a assinatura com selo de tempo (*timestamp*), pelo que a assinatura criada pelo SCMD não contém a hora da sua criação e deste modo não pode ser utilizada, por si só, como prova de que o documento existia e foi assinado antes de determinado prazo.

Após a assinatura ser adicionada ao documento, esta pode ser validada a qualquer altura.

O SCMD está dimensionado para assinar um número significativo de documentos por dia.

3.1.2 PAN (b): Dados a serem assinados

É da responsabilidade das aplicações (identificadas na secção 1.2.2) apresentar os dados a serem assinados no formato XML (que contém o hash do documento a assinar em formato byte array) – também designado por representação dos dados a serem assinados (DTBS/R) –, garantindo que corresponde aos dados/documento a assinar apresentado (conforme indicado na secção 3.2.4) ao assinante.

3.1.3 PAN (c): Relação entre os dados assinados e a(s) assinatura(s)

Cada assinatura criada corresponde ao dado a ser assinado recebido (conforme indicado na secção 3.1.2).

O SCMD cria a assinatura utilizando o algoritmo de assinatura sha256WithRSAEncryption. Esta assinatura é efetuada sobre os dados a serem assinados recebidos (*hash* do documento a assinar), e é devolvida (em formato Base 64) à aplicação que enviou os dados a serem assinados. É da responsabilidade das aplicações (identificadas na secção 1.2.2) guardar a assinatura embebida no documento assinado com os dados assinados ou, guardar a assinatura separada dos dados assinados. A guarda da assinatura é efetuada no formato, perfil e nível de assinatura definida pela aplicação (por exemplo, PAdES Basic, PAdES-EPES, ...), sendo que o formato/perfil/nível utilizado deve permitir adicionar uma referência à Política CMD de Assinatura Qualificada (indicando pelo menos o seu OID), de modo a permitir que partes confiantes e outras pessoas interessadas possam encontrar informação sobre as políticas e práticas seguidas na aposição da assinatura.

O SCMD guarda a representação dos dados a serem assinados (DTBS/R) e a respetiva assinatura e certificado, até um ano após a revogação ou cancelamento do respetivo certificado qualificado CMD.

3.1.4 PAN (c): Utilizadores

A assinatura digital qualificada pode ser efetuada através do SCMD, por cidadão com idade igual ou superior a 16 anos que não se encontre interdito ou inabilitado, e que tenha solicitado a ativação do certificado qualificado CMD para assinatura eletrónica qualificada do cidadão, de acordo com:

- o número 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, e
- o artigo 2º (Registo) da Portaria CMD[3].

3.1.5 PAN (e): Atribuição de responsabilidade pela validação e aumento da assinatura

O SCMD não disponibiliza processos de aumento de assinatura.

A correta verificação da validade da assinatura é da responsabilidade das terceiras partes confiantes nas assinaturas "server-side" criadas pelo SCMD.

3.2 PANs influenciados pelas disposições legais/regulamentares associadas ao processo de negócio/aplicação

3.2.1 PAN (f): Tipo jurídico das assinaturas

A assinatura digital criada pelo SCMD é uma assinatura qualificada eletrónica, como definido na legislação europeia, nomeadamente no regulamento 910/2014 (eIDAS).

3.2.2 PAN (g): Compromisso assumido pelo assinante

O assinante cria a assinatura, através do SCMD, estando a chave de assinatura sob o controlo exclusivo do titular da mesma (i.e., do assinante). Com a assinatura dos dados/documento, o assinante deve associar um (ou vários) dos seguintes tipo de compromissos, de modo a contextualizar (e desambiguar) o propósito e significado da assinatura, assim como a natureza da responsabilidade assumida:

- Prova de origem / *Proof of origin*
    - Significado: indica que o assinante reconhece ter criado, aprovado e enviado os dados assinados.
    - OID: id-cti-ets-proofOfOrigin OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti(6) 1}
    - URI: http://uri.etsi.org/01903/v1.2.2#ProofOfOrigin.

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

- Prova de aprovação / *Proof of approval*
    - Significado: indica que o assinante aprovou o conteúdo dos dados assinados.
    - OID: id-cti-ets-proofOfApproval OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti(6) 5}
    - URI: http://uri.etsi.org/01903/v1.2.2#ProofOfApproval.
- Prova de criação / *Proof of creation*
    - Significado: indica que o assinante criou os dados assinados (não significa necessariamente que os aprovou ou enviou).
    - OID: id-cti-ets-proofOfCreation OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti(6) 6}
    - URI: http://uri.etsi.org/01903/v1.2.2#ProofOfCreation.
- Autenticação de dados / *Data Autentication*
    - Significado: indica que a assinatura foi criada com a intenção de autenticar os dados assinados.
    - OID: 2.16.620.2.1.3.1 – OBJECT IDENTIFIER ::= { joint-iso-itu-t(2) country(16) pt(620) ama(2) scmd(1) cti(3) 1 }
- Autenticação de Entidade / *Entity Autentication*
    - Significado: indica que a assinatura foi criada com a intenção de autenticar a entidade que assina.
    - OID: 2.16.620.2.1.3.2 – OBJECT IDENTIFIER ::= { joint-iso-itu-t(2) country(16) pt(620) ama(2) scmd(1) cti(3) 2 }
- Autoria / *Authorship*
    - Significado: indica que a assinatura foi criada com a intenção de indicar autoria dos dados assinados.
    - OID: 2.16.620.2.1.3.3 – OBJECT IDENTIFIER ::= { joint-iso-itu-t(2) country(16) pt(620) ama(2) scmd(1) cti(3) 3 }
- Revisão / *Review*
    - Significado: indica que a assinatura foi criada com a intenção de indicar a revisão dos dados assinados.
    - OID: 2.16.620.2.1.3.4 – OBJECT IDENTIFIER ::= { joint-iso-itu-t(2) country(16) pt(620) ama(2) scmd(1) cti(3) 4 }
- Cópia / *Copy*
    - Significado: indica que a assinatura foi criada com a intenção de indicar que o documento é uma cópia do original (em papel ou eletrónico).
    - OID: 2.16.620.2.1.3.5 – OBJECT IDENTIFIER ::= { joint-iso-itu-t(2) country(16) pt(620) ama(2) scmd(1) cti(3) 5 }
- Testemunha de assinatura / *Signature Witness*
    - Significado: indica que a assinatura foi criada com a intenção de indicar que o assinante é testemunha que a(s) pessoa(s) que assinaram os mesmos dados com o OID 2.16.620.2.1.3.7, leram, aprovaram e estão vinculados ao conteúdo dos dados assinados.

- OID: 2.16.620.2.1.3.6 – OBJECT IDENTIFIER ::= { joint-iso-itu-t(2) country(16) pt(620) ama(2) scmd(1) cti(3) 6 }

- Vinculação ao conteúdo assinado / *Bound to data signed*
  - Significado: indica que a assinatura foi criada com a intenção de indicar que o assinante leu, aprovou e está vinculado ao conteúdo dos dados assinados.
  - OID: 2.16.620.2.1.3.7 – OBJECT IDENTIFIER ::= { joint-iso-itu-t(2) country(16) pt(620) ama(2) scmd(1) cti(3) 7 }
- Aprovação intermédia / *Intermediate approval*
  - Significado: indica que a assinatura foi criada com a intenção de indicar uma aprovação intermédia, como parte de um processo de decisão.
  - OID: 2.16.620.2.1.3.8 – OBJECT IDENTIFIER ::= { joint-iso-itu-t(2) country(16) pt(620) ama(2) scmd(1) cti(3) 8 }

O(s) tipo(s) de compromisso deve(m) ser selecionado(s)/indicado(s) pelo assinante, de modo a serem adicionados à assinatura. A descrição explícita do(s) compromisso(s) assumido(s) pelo assinante ao assinar o documento, evita ambiguidades potenciais que podem levar à incerteza sobre a intenção do assinante – confiar na informação contextual implícita é uma atitude arriscada.

3.2.3 PAN (h): Nível de garantia das evidências temporais

O SCMD não aumenta a assinatura com selo de tempo (*timestamp*), pelo que a assinatura criada pelo SCMD não contém a hora da sua criação.

3.2.4 PAN (i): Formalidades da assinatura

A interface das aplicações (identificadas na secção 1.2.2) utilizadas pelos assinantes devem ser construídas de forma a satisfazer, na medida do possível, os requisitos legais sobre a expressão de vontade ou intenções dos assinantes. É desse modo importante descrever e especificar a forma como as evidências são construídas no que diz respeito à expressão da vontade ou intenção do signatário de assinar e, em particular, os requisitos relacionados à forma como a atenção do signatário é atraída para a importância do compromisso que está a tomar ao executar o ato de assinar.

Estas aplicações têm os seguintes requisitos:

- Comunicar com o SCMD, em conformidade com o protocolo SAP (cf. secção 3 da "Declaração de Práticas de Operação");
- Apresentar os dados a assinar de acordo com a política WYSIWYS (*What You See Is What You Sign*), diretamente na aplicação ou em aplicação externa;
- Permitir, sempre que adequado, que o assinante identifique qual o compromisso que assume na assinatura dos dados/documento, conforme secção 3.2.2, adicionando tal informação ao campo "Razão"/"*Reason*" da assinatura, assim como deve adicionar o(s) respetivo(s) OID(s) ao campo apropriado da assinatura;
- Possibilitar que o assinante valide 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* da aplicação;
- Identificar e informar sobre os vários passos do processo de assinatura;

- Identificar claramente o passo a partir do qual a assinatura será criada, garantindo que o assinante conhece a responsabilidade assumida no ato de assinar e que fica vinculado a essa responsabilidade e ao compromisso assumido;
- Guiar o assinante na guarda da assinatura embebida no documento assinado com os dados assinados ou, na guarda da assinatura separada dos dados assinados.

3.2.5 PAN (j): Longevidade e resiliência à mudança

O SCMD não aumenta a assinatura com informação que amplie a sua longevidade, pelo que a validade da assinatura termina aquando da expiração da validade do certificado qualificado CMD do assinante.

3.2.6 PAN (k): Arquivo

Não existem requisitos específicos.

3.3 PANs relacionados com os atores envolvidos na criação/aumento/validação das assinaturas

3.3.1 PAN (l): Identidade (e papéis / atributos) dos assinantes

O assinante é um cidadão com idade igual ou superior a 16 anos que não se encontre interdito ou inabilitado, de acordo com o número 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.

No SCMD o assinante assina no papel de cidadão e o certificado contém vários atributos que o qualificam: nome, nacionalidade, data de nascimento, e número de identificação civil.

3.3.2 PAN (m): Nível de confiança exigido para a autenticação do assinante

A subscrição do SCMD e validação inicial do cidadão (assinante/titular do par de chaves) garantem um elevado nível de confiança na identificação e autenticação do cidadão.

Sempre que é efetuado o processo de criação de assinatura, a autenticação do assinante garante um elevado nível de confiança 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.

3.3.3 PAN (n): Dispositivos de criação de assinatura

O SCMD utiliza um dispositivo remoto de criação de assinatura (remote SCDev – Signature Creation Device – na nomenclatura anglo-saxónica).

3.4 Outros PANs

3.4.1 PAN (o): Outra informação a ser associada com a assinatura

O formato/perfil/nível de assinatura utilizado deve permitir adicionar uma referência à Política CMD de Assinatura Qualificada (indicando pelo menos o seu OID), de modo a permitir que partes confiantes e outras pessoas interessadas possam encontrar informação sobre as políticas e práticas seguidas na aposição da assinatura.

3.4.2 PAN (p): Criptografia

O algoritmo de assinatura ("*signature suite*") utilizado na geração da assinatura (indicado na secção 3.1.3) tem a segurança suficiente para a longevidade máxima expectável (indicada na secção 3.2.5).

3.4.3 PAN (q): Ambiente tecnológico

O ambiente tecnológico utilizado é o adequado para um sistema confiável para assinatura "*server-side*" (TW4S).

4 Requisitos / declarações sobre mecanismos técnicos e implementação

4.1 Contraparte técnica dos PANs - Resumo da declaração

A tabela seguinte sumariza os requisitos dos parâmetros no âmbito de negócio (PAN) identificados na secção 3 e, especifica os correspondentes mecanismos técnicos e standards que os implementam.

Nome e identificador da autoridade da Política de assinatura: AMA – Agência para a Modernização Administrativa, I.P. (AMA) **Nome e identificador da Política de assinatura**: Política CMD de assinatura qualificada (2.16.620.2.1.2.2)			
PAN	**Título**	**Sumário da declaração de negócio**	**Correspondente declaração técnica**
(a)	*Workflow* (sequência e *timing*) das assinaturas	No processo de negócio do SCMD apenas é criada uma assinatura por cada DTBS/R recebido, pelo que não existe um *workflow* de assinatura com uma determinada sequência e *timing*. Após a assinatura ser adicionada ao documento, esta pode ser validada a qualquer altura.	A criação da assinatura é efetuada, em HSM no *remote SCDev*, após a receção do código de segurança, em conformidade com o protocolo SAP (cf. secção 3 da "Declaração de Práticas de Operação"). Validação efetuada através da lista de certificados revogados (LCR) ou serviço OCSP (preferencialmente). A URI destes métodos está incluída no certificado digital do titular / assinante (incluído na assinatura digital qualificada), de modo a que a validação possa ser efetuada por mecanismos automáticos.

		O SCMD está dimensionado para assinar um número significativo de documentos por dia.	Utiliza dispositivos criptográficos de assinatura desenhados para assinatura em massa (HSM).
(b)	Dados a serem assinados	As aplicações que permitem que os assinantes efetuem a criação de assinaturas qualificadas através do SCMD, são responsáveis por submeterem os dados a serem assinados (*hash* do documento) ao SCMD, garantindo que corresponde ao documento a assinar apresentado pelo assinante.	Os dados a serem assinados (DTBS/R) são comunicados em formato XML, que contém o *hash* do documento a assinar em formato *byte array*.
(c)	Relação entre os dados assinados e a(s) assinatura(s)	Cada assinatura criada corresponde ao dado a ser assinado recebido. O SCMD efetua a assinatura sobre os dados a serem assinados que recebeu, e devolve-a à aplicação que enviou os dados a serem assinados. É da responsabilidade das aplicações (identificadas na secção 1.2.2) guardar a assinatura embebida no documento assinado com os dados assinados ou, guardar a assinatura separada dos dados assinados.	Não existe ao nível do SCMD nenhum mecanismo para assinatura duplicada, em que para um dado a ser assinado recebido, seja criada mais do que uma assinatura. O SCMD cria a assinatura sobre o *hash* do documento a assinar, utilizando o algoritmo de assinatura sha256WithRSAEncryption e, devolve-a em formato Base 64 à aplicação que enviou o correspondente DTBS/R.
(d)	Utilizadores	A assinatura digital qualificada pode ser efetuada através do SCMD, por cidadão com idade igual ou superior a 16 anos que não se encontre interdito ou inabilitado, e que tenha solicitado a ativação do certificado qualificado CMD para assinatura eletrónica qualificada do cidadão.	A idade, interdição e/ou inabilitação é validado automaticamente na ativação do certificado qualificado CMD, através do Cartão de Cidadão e serviços dos organismos relevantes para a validação de interdição e inabilitação.

(e)	Atribuição de responsabilidade pela validação e aumento da assinatura	O SCMD não disponibiliza processos de aumento de assinatura. A correta verificação da validade da assinatura é da responsabilidade das terceiras partes confiantes em assinaturas "server-side" criadas pelo SCMD.	As terceiras partes confiantes 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; • Conhecer e aceitar as Políticas associadas à assinatura em que confia.
(f)	Tipo jurídico das assinaturas	A assinatura digital criada pelo SCMD é uma assinatura qualificada eletrónica, como definido na legislação europeia, nomeadamente no regulamento 910/2014 (eIDAS).	O SCMD está conforme com o regulamento 910/2014 (eIDAS) e com o despacho 155/2017 do Gabinete Nacional de Segurança.
(g)	Compromisso assumido pelo assinante	Com a assinatura dos dados/documento, o assinante deve associar um (ou vários) tipo de compromissos, de modo a contextualizar (e desambiguar) o propósito e significado da assinatura, assim como a natureza da responsabilidade assumida. O(s) tipo(s) de compromisso deve(m) ser	O(s) tipo(s) de compromisso deve(m) ser adicionado(s) na língua do assinante e em inglês, ao campo "Razão"/"*Reason*" da assinatura, devendo a aplicação utilizada colocar o(s) respetivo(s) OID(s) no campo apropriado da assinatura.

		selecionado(s)/indicado(s) pelo assinante, de modo a serem adicionados à assinatura.	
(h)	Nível de garantia das evidências temporais	O SCMD não aumenta a assinatura com selo de tempo (*timestamp*), pelo que a assinatura criada pelo SCMD não contém a hora da sua criação.	O SCMD regista e guarda a hora exata em que a assinatura é criada, estando a hora, em toda a infraestrutura SCMD, 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[4] em que o desvio máximo para o UTC[5] é de um segundo.
(i)	Formalidades da assinatura	A interface das aplicações (identificadas na secção 1.2.2) utilizadas pelos assinantes devem ser construídas de forma a satisfazer, na medida do possível, os requisitos legais sobre a expressão de vontade ou intenções dos assinantes.	As aplicações devem satisfazer tecnicamente os requisitos apresentados na secção 3.2.4.
(j)	Longevidade e resiliência à mudança	O SCMD não aumenta a assinatura com informação que amplie a sua longevidade, pelo que a validade da assinatura termina aquando da expiração da validade do certificado qualificado CMD do assinante.	O certificado digital do assinante está incluído na assinatura digital qualificada, de modo a que a verificação da validade do certificado possa ser efetuada por mecanismos automáticos.
(k)	Arquivo	Não existem requisitos específicos.	Não existem requisitos específicos.

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

(l)	Identidade (e papéis / atributos) dos assinantes	No SCMD o assinante assina no papel de cidadão e o certificado contém vários atributos que o qualificam: nome, nacionalidade, data de nascimento, e número de identificação civil.	Os atributos encontram-se nos seguintes campos do *Subject* do certificado qualificado CMD: • *Common Name* – contém o nome completo do assinante; • *Surname* – contém o(s) nome(s) de família do assinante; • *Given Name* – contém o(s) nome(s) próprio do assinante; • *Serial Number* – constituído por "<Número do documento de identificação do Cidadão>". A data de nascimento, quando exista, encontra-se no campo "*Subject directory attributes*" (sub-campo "*Date of Birth*") do certificado qualificado CMD.
(m)	Nível de confiança exigido para a autenticação do assinante	A subscrição do SCMD e validação inicial do cidadão (assinante/titular do par de chaves) garantem um elevado nível de confiança na identificação e autenticação do cidadão.	Na ativação/emissão do certificado qualificado CMD (e consequente subscrição do SCMD) do assinante é garantido 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[6] Clause 2.1;

[6] *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.*

		Sempre que é efetuado o processo de criação de assinatura, a autenticação do assinante garante um elevado nível de confiança 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.	• As características do meio eletrónico de identificação estão conforme a *assurance level high* na componente "*Electronic identification means characteristics and design*" – (EU) 2015/1502[6] Clause 2.2.1; • O mecanismo de autenticação está conforme a *assurance level high* da (EU) 2015/1502[6] Clause 2.3.1. A autenticação do assinante segue o protocolo de ativação de assinatura SAP (cf. secção 3 da "Declaração de Práticas de Operação").
(n)	Dispositivos de criação de assinatura	O SCMD utiliza um dispositivo remoto de criação de assinatura (remote SCDev – Signature Creation Device – na nomenclatura anglo-saxónica).	O *remote* SCDev é um SCDev (concretizado num dispositivo HSM com certificação FIPS 140-2 nível 3 e/ou *Common Criteria* EAL 4+) 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). 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* num *filesystem* externo, localizado fisicamente numa máquina protegida contra adulteração.

(o)	Outra informação a ser associada com a assinatura	A assinatura deve 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.	A referência à Política CMD de Assinatura Qualificada deve conter pelo menos o OID da mesma, e deve ser colocado no local mais apropriado, de acordo com o formato/perfil/nível de assinatura utilizado, garantindo, sempre que possível, a visualização da mesma pelo leitor do documento, assim como a sua obtenção automática por software de processamento de documentos.
(p)	Criptografia	O algoritmo de assinatura ("*signature suite*") utilizado na geração da assinatura tem a segurança suficiente para a longevidade máxima expectável.	A assinatura é efetuada no HSM, utilizando o algoritmo de assinatura ("*signature suite*") sha256WithRSAEncryption.
(q)	Ambiente tecnológico	O ambiente tecnológico utilizado é o adequado para um sistema confiável para assinatura "*server-side*" (TW4S).	O ambiente tecnológico segue as recomendações indicadas no despacho 155/2017 do Gabinete Nacional de Segurança, tal como descrito na secção 6.2 da "Declaração de Práticas de Operação".
Declarações de práticas de aplicação de assinatura		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.	Os mecanismos técnicos, requisitos e standards que os implementam devem ser consultados no documento "Declaração de Práticas de Operação".

4.2 Restrições de *input* e *output* para procedimentos de criação, aumento e validação de assinaturas

4.2.1 Restrições de *input* a serem usadas ao gerar, aumentar e/ou validar assinaturas no contexto da política de assinatura

A tabela seguinte tem por base a tabela da secção 4.1 (que deverá ser consultada para informação do sumário da declaração de negócio e correspondente declaração técnica para cada um dos PAN), complementando-a com as restrições que podem ser parametrizadas com base nos PANs ao nível da criação, aumento e validação de assinatura, e identificando se tais restrições se referem à *driving application* (SCA), aplicação de criação de assinatura (SSA) e/ou aplicação de validação de assinatura (SVA), incluindo a valoração dessas restrições.

Sempre que restrições se referem à SCA ou SVA, essas são medidas/requisitos que os fornecedores de SCA e SVA para as assinaturas SCMD têm que seguir e/ou validar.

Como o SCMD não disponibiliza processos de aumento de assinatura, a tabela não reflete valores da restrição no aumento da assinatura.

Nome e identificador da autoridade da Política de assinatura: AMA – Agência para a Modernização Administrativa, I.P. (AMA) **Nome e identificador da Política de assinatura**: Política CMD de assinatura qualificada (2.16.620.2.1.2.2)				
PAN	**Título**	**Restrições**	**Valor da restrição na criação da assinatura** (SSA ou SCA)	**Valor da restrição na validação da assinatura** (SVA ou SCA)
(a)	*Workflow* (sequência e *timing*) das assinaturas	OrderInSequence (Ordem na sequência)	n/a	n/a (não aplicável)
		SequencingNature (Natureza da Sequência)	Mandated-independent (SSA)	n/a
		TimingRelevance (Relevância do *timing*)	n/a	n/a

		MassSigningAcceptable (Aceitação de assinatura em massa)	Sim (SSA)	n/a
(b)	Dados a serem assinados	ConstraintOnDTBS (Restrição nos dados a serem assinados)	Não existem restrições no tipo de dados a serem assinados.	n/a
		ContentRelatedConstraints AsPartOfSignatureElements (Restrição relacionada com o conteúdo dos elementos de assinatura)	MandatedSignedQProperties-DataObjetFormat: XML que contém o *hash* do documento a assinar.	n/a
		DOTBSAsAWholeOrInParts (Dados a serem assinados, assinados na totalidade ou em parte)	parts: será apenas assinada a *hash* do documento a assinar contida no XML.	n/a
(c)	Relação entre os dados assinados e a(s) assinatura(s)	BulkSigningRelevance (Relevância da assinatura em massa)	mandatedBulkSigning: O XML enviado pela SCA pode conter as *hashs* de vários documentos a assinar.	n/a
		ConstraintsOnTheNumberOfDOTBS (Restrição no número de dados a serem assinados)	1 (um) – cada *hash* é assinada pela chave privada do assinante, pelo que uma assinatura serve para assinar apenas uma *hash* submetida (i.e., um documento).	n/a
		SignatureRelativePosition (Posição relativa da assinatura)	Não está predeterminado, sendo responsabilidade da SCA.	n/a
		MandatedSignatureFormat (Formato da Assinatura)	SSA: assinatura utiliza o algoritmo de assinatura sha256WithRSAEncryption e, devolve-a em formato Base 64 à SCA.	n/a

			SCA: Não está predeterminado o formato/perfil/nível em que a assinatura é guardada, sendo tal da responsabilidade da SCA.	
(d)	Utilizadores	TargetedCommunityConstraints (Restrições na comunidade alvo)	Cidadão com idade igual ou superior a 16 anos que não se encontre interdito ou inabilitado (SSA)	n/a
(e)	Atribuição de responsabilidade pela validação e aumento da assinatura	ValidationRequiredBeforeAugmenting (Necessidade de validação antes de aumento da assinatura)	n/a	n/a
		AugmentToLevel (Nível a atingir após aumento da assinatura)	n/a	n/a
(f)	Tipo jurídico das assinaturas	ConstraintsOnCertificateMetadata (Restrições nos metadatos dos certificados)	EUQualifiedCertificateSigRequired, EUQSigCDRequired	
(g)	Compromisso assumido pelo assinante	CommitmentTypesRequired (Tipos de compromissos necessários)	• MandatedSignedQProperties-commitment-type-indication: false, • MandatedCommitmentTypeValues: MatchingValuesIndicator: "none" • MandatedCommitmentTypeValues: CommitmentTypeValues: { {1.2.840.113549.1.9.16.6.1, Prova de origem / *Proof of origin*}, {1.2.840.113549.1.9.16.6.5, Prova de aprovação / *Proof of approval*}, {1.2.840.113549.1.9.16.6.6, Prova de criação / *Proof of creation*}, {2.16.620.2.1.3.1, Autenticação de dados / *Data Autentication*}, {2.16.620.2.1.3.2, Autenticação de Entidade / *Entity Autentication*}, {2.16.620.2.1.3.3, Autoria / *Authorship*}, {2.16.620.2.1.3.4, Revisão / *Review*}, {2.16.620.2.1.3.5, Cópia / *Copy*}, {2.16.620.2.1.3.6, Testemunha de	

			assinatura / *Signature Witness*}, {2.16.620.2.1.3.7, Vinculação ao conteúdo assinado / *Bound to data signed*}, {2.16.620.2.1.3.8, Aprovação intermédia / *Intermediate approval*} }	
(h)	Nível de garantia das evidências temporais	LoAOnTimingEvidences (Nível de garantia das evidencias temporais)	n/a	LoA-on-time-in-OCSP-response: inferior a 1 segundo (SCA, SVA) LoA-on-time-in-CRL: inferior a 1 segundo (SCA, SVA)
(i)	Formalidades da assinatura	WYSIWYSRequired (WYSIWYS necessário)	Verdadeiro (SCA)	n/a
		WYSIWHBSRequired (WYSIWHBS[7] necessário)	Falso (SCA)	n/a
		ProperAdviceAndInformationRequired (Necessário fornecer a assinante informação e conselho relativo ao processo de criação de assinatura e consequências legais, assim como garantir na extensão possível, que o interface do utilizar fornece um ambiente legal válido para assinatura)	Verdadeiro (SCA)	n/a
		UserInterfaceDesignConstraints (Restrições no desenho do interface do utilizador, conforme identificado na secção 3.2.4)	Verdadeiro (SCA)	n/a

[7] WYSIWHBS - "what you see is what has been signed"

		CorrectValidationAndArchivalProcedures (Indicação do procedimento de arquivo/validação, conforme identificado na secção 3.2.4)	Verdadeiro (SCA)	n/a
(j)	Longevidade e resiliência à mudança	LoAOnLongevityAndResilience (Nível de garantia de longevidade e resiliência)	Validade da assinatura termina aquando da expiração do certificado qualificado CMD do assinante.	
(k)	Arquivo	ArchivalConstraints (Requisitos para arquivo da assinatura e dados de validação associados)	n/a	n/a
(l)	Identidade (e papéis / atributos) dos assinantes	ConstraintsOnCertificateMetadata-LegalPersonSignerRequired	n/a	n/a
		ConstraintsOnCertificateMetadata-LegalPersonSignerAllowed	n/a	n/a
		MandatedSignedQProperties-signer-attributes	n/a	n/a
		NameConstraints	O *Distinguished Name* do certificado do assinante segue o seguinte formato: C = "PT", O = "Cartão de Cidadão", OU = "Cidadão", OU = "Chave Móvel Digital de Assinatura Qualificada do Cidadão", OU = "RemoteQSCDManagement", CN = <concatenação do *givenName* e *SN* do Cidadão>, SN = <nome de família	O *Distinguished Name* do emissor da lista de revogação de certificados (tanto da LRC como da delta LRC) segue o seguinte formato: C = "PT", O = "Cartão de Cidadão", OU = "subECEstado", CN = "EC de Chave

			do Cidadão>, givenName = <parte do nome do Cidadão que não é o nome de família nem os nomes intermédios>, serialNumber = <Número do documento de identificação do Cidadão >. O "*Subject directory attributes*" (sub-campo "*Date of Birth*") pode conter a data de nasimento do assinante. (SCA, SSA)	Móvel Digital de Assinatura Qualificada do Cartão de Cidadão <nnnn>[8]". O *Distinguished Name* do titular do certificado do *OCSP responder* segue o seguinte formato: C = "PT", O = "Cartão de Cidadão", OU = "Serviços do Cartão de Cidadão", OU = "Validação on-line", CN = "Serviço de Validação on-line do Cartão de Cidadão <nnnnnn>[8] - EC de Chave Móvel Digital de Assinatura Qualificada".
(m)	Nível de confiança exigido para a autenticação do assinante	X509CertificateValidationConstraints (requisitos para usar no processo de validação da hierarquia de confiança do certificado de assinatura, de acordo com o IETF RFC 5280)	SetOfTrustAnchors: a raiz de confiança da hierarquia onde é emitido o certificado de assinatura, certificado OCSP e lista de revogação de certificados, é o certificado da EC do Cartão de Cidadão (https://webgate.ec.europa.eu/tl-browser/#/tl/PT/1), certificado da EC da ECCE (https://webgate.ec.europa.eu/tl-browser/#/tl/PT/4), ou certificado da EC CMD (https://webgate.ec.europa.eu/tl-browser/#/tl/PT/), disponibilizado numa *Trust Service Status Lists* (TSL) conforme ETSI TS 102 231, em que o "*Service Type Identifier*" é o *qualified trust service type* CA/QC.	
		RevocationConstraints (requisitos aplicáveis na validação do estado dos certificados no processo de validação da	n/a	RevocationCheckingConstraints: ocspCheck RevocationFreshnessConstraints: 2 segundos no caso do OCSP;

[8] Número sequencial começado em 1 (pode ter um ou mais zeros a preceder o número).

		hierarquia de confiança do certificado de assinatura)		FreshestCRL ou deltaCRL no caso da lista de revogação de certificados.
		LoAOnTSPPractices (Nível de garantia das práticas dos TSP(s) que emitiram certificados da hierarquia de confiança do certificado de assinatura)	Todos os TSPs que emitiram certificados da hierarquia de confiança do certificado de assinatura têm de ser "prestadores qualificados de serviços de confiança", de acordo com o regulamento EU 910/2014.	
(n)	Dispositivos de criação de assinatura	LoAOnSCD (Nível de garantia dos dispositivos de criação de assinatura onde residem as chaves privadas correspondentes aos certificados validados no processo de validação da hierarquia de confiança do certificado de assinatura)	Todos os dispositivos de criação de assinatura têm que ser "dispositivos qualificados de criação de assinaturas eletrónicas", de acordo com o regulamento EU 910/2014.	
(o)	Outra informação a ser associada com a assinatura	MandatedSignedQProperties-signer-location	n/a	n/a
		MandatedUnsignedQProperties-signature-policy-extension	Sempre que o formato/perfil/nível de assinatura o permitir, a *signature policy extension* deve ser utilizada para conter pelo menos o OID da Política CMD de Assinatura Qualificada.	
		MandatedUnsignedQProperties-signature-policy-inclusion-inarchival-form	n/a	n/a
(p)	Criptografia	CryptographicSuitesConstraints	As restrições sobre os algoritmos e parâmetros utilizados nos certificados de assinatura e na criação da assinatura	As restrições sobre os algoritmos e parâmetros utilizados pelo OCSP responder e nas listas de revogação

			encontram-se na próxima tabela (SCA, SSA)	encontram-se na próxima tabela (SCA, SVA)
(q)	Ambiente tecnológico	TechnologicalEnvironmentConstraints	Os requisitos do ambiente tecnológico em que as assinaturas são processadas segue as recomendações indicadas no despacho 155/2017 do Gabinete Nacional de Segurança, tal como descrito na secção 6.2 da "Declaração de Práticas de Operação".	n/a
O formato da assinatura é da responsabilidade da SCA, devendo ser selecionado um formato standard que permita adicionar uma referência à Política CMD de Assinatura Qualificada (indicando pelo menos o seu OID), de modo a permitir que partes confiantes e outras pessoas interessadas possam encontrar informação sobre as políticas e práticas seguidas na aposição da assinatura.				

(p) Criptografia				
Tipo de assinatura	**Identificador de algoritmo**	**Tamanho mínimo da chave de assinatura**	**Tamanho mínimo do hash**	**Data de expiração**
Assinatura a validar	sha256WithRSAEncryption	2048 bits	256 bits	Até ao fim da validade do certificado do assinante utilizado na assinatura.
Certificado do assinante	sha256WithRSAEncryption	2048 bits	256 bits	Até 10 anos.
Certificado da EC numa cadeia de certificação válida	sha256WithRSAEncryption	2048 bits	256 bits	Até 12 anos.

Resposta OCSP	sha256WithRSAEncryption	2048 bits	256 bits	Até ao fim da validade do certificado que assinou a resposta OCSP.
Lista de revogação de certificados	sha256WithRSAEncryption	2048 bits	256 bits	Até à emissão da próxima CRL ou deltaCRL.

4.2.2 Restrições de *output* a serem usadas ao validar assinaturas no contexto da política de assinatura

Não existem restrições ou requisitos, derivados dos PANs, aplicáveis ao output do procedimento de validação de assinatura SCMD.

4.2.3 Restrições de *output* a serem usadas ao gerar/aumentar assinaturas no contexto da política de assinatura

Não existem restrições ou requisitos, derivados dos PANs, aplicáveis ao output do procedimento de geração de assinatura SCMD. O SCMD não disponibiliza mecanismos de aumento de assinatura SCMD.

5 Outros assuntos comerciais e legais

Ver capítulo com o mesmo nome da "Declaração de Práticas de Operação".

6 Auditoria de conformidade e outras avaliações

Ver capítulo com o mesmo nome da "Declaração de Práticas de Operação".

Aprovação

Aprovado pelo Grupo de Trabalho de Gestão.

Assinado por : **ANDRÉ FERREIRA FERRÃO COUTO E VASCONCELOS**
Num. de Identificação Civil: BI111164753
Data: 2018.06.19 19:27:54 GMT Daylight Time

Assinado por : **RITA SUZINDA LOURENÇO PINTO REI**
Num. de Identificação Civil: BI102699577
Data: 2018.06.19 21:37:14 Hora de Verão de GMT