AUTENTICAÇÃO.GOV
CHAVE MÓVEL DIGITAL

Declaração de Divulgação de Princípios da EC CMD

Políticas (POL#21)

Nível de Acesso: Público

Versão: 2.0

Data: Mar/2022

AMA – Agência para a Modernização Administrativa, I.P.
Rua de Santa Marta n.º 55 1150 - 294, Lisboa, Portugal
Telefone: +351 217 231 200 e-mail: ama@ama.pt

Identificador do Documento: POL#21

Palavras-chave: PKI CMD, Chave Móvel Digital, Divulgação de Princípios

Tipologia Documental: Políticas

Título: Declaração de Divulgação de Princípios da EC CMD

Nível de acesso: Público

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

Data: Mar/2022

Versão atual: 2.0

Validade do Documento: 2 (dois) anos após a sua aprovação.

Histórico de Versões

Versão	Data	Detalhes
1.0	Fev/2018	Versão aprovada.
2.0	Mar/2022	Versão aprovada após revisão.

Documentos Relacionados

Documento	Autor	Descrição
Política de Certificados da EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão (POL#25 – EC CMD)	AMA	Descreve a Política de Certificados da EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão, identificando os perfis de certificado e LCR emitidos, assim como a resposta OCSP.
Declaração de Práticas de Certificação da EC de Chave Móvel Digital de Assinatura Qualificada do Cartão de Cidadão (POL#30 – EC CMD)	AMA	Descreve os procedimentos e práticas utilizados pela EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão para suportar a sua atividade de emissão de certificados qualificados.
Política CMD de Assinatura Qualificada (POL#16 – SCMD)	AMA	Política de assinatura qualificada, de acordo com o ETSI TS 119 172 – 1, adaptada ao SCMD.
Condições gerais de utilização do serviço SCMD (POL#8 – 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. Inclui condições de utilização do certificado qualificado CMD, onde constam os procedimentos necessários em caso de expiração, revogação e renovação do certificado, bem como os termos, condições e âmbito de utilização do mesmo.

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, 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

Este documento resume (mas não substitui), de forma simples e acessível, as características descritas nas Políticas de Certificado (POL#25 – EC CMD) e Declaração de Políticas de Certificação (POL#30 – EC CMD) da EC de Chave Móvel Digital de Assinatura Qualificada do Cartão de Cidadão (disponíveis no repositório do SCMD[1]). É elaborado tendo em conta as especificações técnicas indicadas no anexo A da norma ETSI 319 411-1[2].

A EC de Chave Móvel Digital de Assinatura Qualificada do Cartão de Cidadão (ou Entidade de Certificação CMD) promove a segurança eletrónica do Cidadão no seu relacionamento com o Estado, ao estabelecer uma estrutura de confiança eletrónica que proporciona a realização de transações eletrónicas seguras, assegurando a autoria, integridade e não repúdio de transações ou informação, através de certificado qualificado de assinatura eletrónica, emitido por prestador qualificado de serviço de confiança (AMA – Agência para a Modernização Administrativa, I.P.), conforme regulamento eIDAS[3].

A hierarquia de confiança da Entidade de Certificação CMD encontra-se englobada na hierarquia da Entidade de Certificação do Cartão de Cidadão e na hierarquia do Sistema de Certificação Eletrónica do Estado Português (SCEE[4]).

A Declaração de Divulgação de Princípios da Entidade de Certificação CMD não constitui uma Política de Certificados sob a qual se regem os certificados emitidos pela mesma. Para este efeito devem ser consultadas as Políticas de Certificados e Declaração de Práticas de Certificação disponíveis em https://pki.cartaodecidadao.pt/.

1.1 Público-Alvo

O público-alvo deste documento são os titulares, e terceiras partes de confiança, de certificados qualificados de assinatura eletrónica, emitidos pela Entidade de Certificação CMD.

[1] Documentos disponibilizados em https://www.autenticacao.gov.pt/web/guest/documentos

[2] ETSI 319 411-1: *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirement.*V1.2.2.

[3] Regulamento eIDAS: 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 e que revoga a Diretiva 1999/93/CE.

[4] https://www.scee.gov.pt/

2 Contactos da Entidade de Certificação CMD

O contacto principal da Entidade de Certificação CMD é o seguinte:

Nome	AMA – Agência para a Modernização Administrativa, I.P.
Morada	Rua de Santa Marta n.º 55 1150 - 294, Lisboa
Correio eletrónico	ama@ama.pt
Telefone	217 231 200

Caso necessite de revogar o certificado qualificado de assinatura eletrónica CMD, o pedido de revogação pode ser efetuado de duas formas alternativas:

- Presencial, nos balcões de atendimento (identificados em https://www.autenticacao.gov.pt/cmd-pedido-chave);
- *Online*, através do serviço AUTENTICAÇÃO.GOV (https://www.autenticacao.gov.pt/), mediante uma das seguintes formas de autenticação:
    - Autenticação com certificado de autenticação do Cartão de Cidadão do titular do certificado de pessoa singular,
    - Autenticação com Chave Móvel Digital de autenticação do titular do certificado de pessoa singular.

Os motivos para revogação encontram-se identificados na "Declaração de Práticas de Certificação da EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão".

3 Tipos de certificados, procedimentos de validação e utilização

A Entidade de Certificação CMD emite os seguintes tipos de certificado qualificado de assinatura eletrónica para pessoa singular (cidadão):

- Certificado qualificado CMD para cidadão, também designado por **certificado qualificado para assinatura CMD.** Pode ser utilizado para assinatura digital qualificada, de acordo com Regulamento (UE) nº 910/2014[3] e Decreto-Lei n.º 12/2021, em que a chave privada se encontra num dispositivo criptográfico QSCD.
- Certificado qualificado CMD para cidadão, em representação de pessoa coletiva, para assinatura de faturas eletrónicas (no âmbito do Serviço de Assinatura de Faturas Eletrónicas – SAFE), também designado por **certificado qualificado para assinatura SAFE**. Pode ser utilizado para assinatura de faturas eletrónicas (e demais documentos fiscalmente relevantes) emitidas pela pessoa coletiva identificada no atributo *Organization* e no atributo *Organization Identifier*, conforme Decreto-Lei n.º 28/2019, de 15 de fevereiro, nos termos do disposto no n.2 do artigo 12.º.

Ambos os certificados qualificados de assinatura eletrónica são emitidos conforme regulamento eIDAS[3] e Decreto-Lei n.º 12/2021, estando cada perfil de certificado identificado no documento "Política de Certificados da EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão[1]". Esta política de certificado é representada no certificado qualificado através de um número único designado de "identificador de objeto" (OID): "2.16.620.1.1.1.2.4.3.0.1.1.

O certificado qualificado de assinatura eletrónica é um meio legalmente aceite para assinar documentos eletrónicos, garante a integridade dos conteúdos assinados, autenticidade da sua assinatura e não repúdio, não podendo negar que assinou determinado conteúdo.

Com o certificado qualificado de assinatura eletrónica, o titular pode efetuar a assinatura eletrónica qualificada de documentos, através de aplicações disponibilizadas e/ou autorizadas pela AMA (identificadas em https://www.autenticacao.gov.pt/web/guest/cmd-assinatura e em https://www.autenticacao.gov.pt/web/guest/serviço-de-assinatura-de-faturas-eletrónicas-safe).

O par de chaves criptográficas associadas ao certificado são gerados e armazenados em ambiente criptográfico seguro pelo prestador qualificado de serviço de confiança (AMA – Agência para a Modernização Administrativa, I.P.), sob o exclusivo controle do titular das mesmas, conforme despacho 155/2017[5] da Entidade supervisora nacional e norma CEN EN 419241-1:2018[6]

O estado de validade dos certificados pode ser verificado através do serviço OCSP (*Online Certificate Status Protocol*) e/ou da consulta das LRC (Listas de Revogação de Certificados), ambos identificados no próprio certificado.

[5] Documento disponível em https://www.gns.gov.pt/media/10445/Despacho-155-2017-Assinaturas%20%C3%A0%20distancia.pdf.

[6] CEN EN 419241-1:2018 *Trustworthy Systems Supporting Server Signing; Part 1: General System Security Requirements*

4 Limites de confiança

O certificado qualificado de assinatura eletrónica tem como objetivo a sua utilização através de aplicações disponibilizadas e/ou autorizadas pela AMA (identificadas em https://www.autenticacao.gov.pt/web/guest/cmd-assinatura e em https://www.autenticacao.gov.pt/web/guest/serviço-de-assinatura-de-faturas-eletrónicas-safe-) para efeitos de assinatura digital qualificada, de acordo com a utilização do tipo/perfil de certificado:

Perfil de certificado	Uso do certificado e par de chaves
Certificado qualificado para assinatura CMD	Utilizado para assinatura digital qualificada, de acordo com Regulamento (UE) nº 910/2014[Error! Bookmark not defined.] e Decreto-Lei n.º 12/2021, em que a chave privada se encontra num dispositivo criptográfico QSCD.
Certificado qualificado para assinatura SAFE	Utilizado para assinatura de faturas eletrónicas (e demais documentos fiscalmente relevantes) emitidas pela pessoa coletiva identificada no atributo *Organization* e no atributo *Organization Identifier*, conforme Decreto-Lei n.º 28/2019, de 15 de fevereiro, nos termos do disposto no n.2 do artigo 12.º.

O Cidadão (pessoa singular) é o titular do certificado qualificado de assinatura eletrónica e encontra-se devidamente identificado pelo nome único (*distinguished name do "Subject"*) no próprio certificado.

Na utilização do certificado e da chave pública, o titular deve garantir o cumprimento das seguintes condições:

a) Ter conhecimento e perceber a utilização e funcionalidades proporcionadas pela criptografia de chave pública e certificados;

b) Ser responsável pela sua correta utilização;

c) Ler e entender os termos e condições descritos nas políticas, práticas de certificação e documentos relacionados indicados neste documento;

d) Verificar os certificados (validação de cadeias de confiança) e Listas de Revogação de Certificados tendo especial atenção às suas extensões marcadas como críticas e propósito das chaves;

e) Confiar nos certificados, utilizando-os sempre que estes estejam válidos.

4.1 Arquivo de informação de registo

A informação de registo e emissão dos certificados é guardada durante sete anos após o fim da validade do respetivo certificado, de acordo com a alínea f) do artigo 13º do Decreto-Lei nº 12/2021.

Os dados pessoais recolhidos para a emissão dos certificados são os dados que constam no próprio certificado, nomeadamente: nome, número de identificação civil e, data de nascimento do cidadão.

5 Responsabilidades do titular do certificado

O certificado identificado na secção 3 (e respetiva chave privada) só pode ser utilizado para o fim a que se destina (conforme estabelecido no campo do certificado "*keyUsage*") e, sempre com propósitos legais. A sua utilização apenas é permitida:

a) A quem estiver designado no campo "*Subject*" do certificado;

b) Após o titular aceitar as "Condições gerais de utilização do serviço SCMD"[1];

c) Enquanto o certificado se mantiver válido e não estiver na Lista de Revogação de Certificados da Entidade de Certificação CMD.

A chave privada associada ao certificado é armazenada em ambiente criptográfico seguro pelo prestador qualificado de serviço de confiança (cf. secção 3) e apenas pode ser utilizada para efeitos de assinatura eletrónica qualificada de documentos, através de aplicações disponibilizadas e/ou autorizadas pela AMA (cf. secção 3), de acordo com a utilização do tipo/perfil de certificado (cf. secção 4).

O certificado identificado na secção 3 (e respetiva chave privada) considera-se aceite pelo titular, após este ter fornecido a palavra-passe de proteção da chave privada no ambiente criptográfico seguro.

O titular do certificado tem obrigação de:

- Fornecer informação correta e completa;
- Utilizar os certificados (e respetiva chave privada) apenas para os fins a que se destinam (cf. secção 3 e secção 4);
- Garantir que a chave privada apenas é utilizada pelo titular do certificado, pelo que se deve abster de partilhar ou divulgar a palavra-passe de proteção da chave privada.

O titular do certificado tem que iniciar o processo de revogação do certificado nas condições identificadas nas "Condições gerais de utilização do serviço SCMD"[1].

A partir do momento em que ocorra uma das situações identificadas para início do processo de revogação do certificado, o titular tem de interromper imediata e permanentemente o uso da respetiva chave privada.

No caso de ser informado que o certificado ou algum certificado na hierarquia de confiança da Entidade de Certificação do Cartão de Cidadão foi revogado ou comprometido, o titular tem de deixar de utilizar a respetiva chave privada.

6 Verificação do estado do certificado por terceiras partes

Terceiras partes que confiam nos certificados emitidos pela Entidade de Certificação do Cartão CMD são responsáveis por:

- Verificar o estado do certificado (ativo, suspenso ou revogado) no momento da sua utilização, através dos mecanismos OCSP e/ou LRC identificados no certificado, e aceitá-lo apenas se estiver dentro do seu período de validade e no estado ativo;
- Aceitar o certificado apenas quando é utilizado para o fim a que se destina (conforme estabelecido no campo do certificado "*keyUsage*");
- Ter em atenção limitações na utilização do certificado, indicadas no próprio certificado ou nas políticas do certificado em causa;
- Ter em atenção outras precauções identificadas em normas, acordos internacionais, legislação ou outros.

A aceitação do certificado é da responsabilidade exclusiva da parte confiante.

7 Limitação de responsabilidades

A Entidade de Certificação CMD:

- Responde pelos prejuízos que cause aos titulares ou a terceiros pela falta ou atraso na inclusão no serviço de consulta sobre a vigência dos certificados, da revogação ou suspensão dum certificado, uma vez que tenha conhecimento dele;
- Só responde pelos danos e prejuízos causados pelo uso indevido do certificado reconhecido, quando não tenha consignado no certificado, de forma clara reconhecida por terceiros o limite quanto ao possível uso.
- A responsabilidade da administração / gestão da Entidade de Certificação CMD 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;
- Não responde se o destinatário dos documentos assinados eletronicamente não os validar e tiver em conta as restrições que figuram no certificado quanto às suas possíveis utilizações;
- Não se responsabiliza pelo uso indevido dos certificados digitais;
- Não se responsabiliza por qualquer utilização dos certificados digitais que não conste na Declaração de Práticas de Certificação ou na Política de Certificados;
- Não assume qualquer responsabilidade no caso de perca ou prejuízo:
    - Dos serviços que presta, em caso de guerra, desastres naturais ou qualquer outro caso de força maior;
    - Ocasionados pelo uso dos certificados quando excedam os limites estabelecidos pelos mesmo na Política de Certificados e correspondente Declaração de Práticas de Certificação:
    - Ocasionado pelo uso indevido ou fraudulento dos certificados ou LRC.

Adicionalmente,

- A utilização dos certificados digitais é da exclusiva responsabilidade do seu titular;
- No âmbito do Serviço de Chave Móvel Digital a chave privada é gerada, armazenada e utilizada em ambiente criptográfico seguro (QSCD – *Qualified Signature Creation Device*) do referido serviço, sob o exclusivo controle do titular da mesma.

8 Acordos aplicáveis, Declaração de Práticas de Certificação e Políticas de Certificação

É aplicável a:

- "Política de Certificados da EC de Assinatura Digital Qualificada do Cartão de Cidadão",
- "Declaração de Práticas de Certificação da EC de Chave Móvel Digital de Assinatura Qualificada do Cartão de Cidadão",
- "Política CMD de Assinatura Qualificada",
- "Condições gerais de utilização do serviço SCMD",

Estes documentos encontram-se disponíveis no repositório do SCMD[1].

9 Política de privacidade

A Entidade de Certificação CMD tem medidas implementadas que garantem a privacidade dos dados pessoais, de acordo com a legislação portuguesa, garantindo que a informação do titular, constante nos respetivos certificados digitais, não se encontra publicada, sendo processada de acordo com a "Política de Certificação do Sistema de Certificação Eletrónica do Estado"[7].

[7] Disponível no repositório https://www.scee.gov.pt/rep/.

10 Indemnizações

De acordo com a legislação em vigor.

11 Legislação aplicável e resolução de conflitos

É aplicável a Lei Portuguesa e os Regulamentos da EU, nomeadamente:

- Regulamento (UE) Nº 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 e que revoga a Diretiva 1999/93/CE;
- Decreto-Lei n.º 12/2021, de 9 de fevereiro de 2021, que assegura a execução na ordem jurídica interna do Regulamento (UE) 910/2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno;
- Lei nº32/2017 de 1 de junho – Segunda alteração à Lei nº7/2007, de 5 de fevereiro, que cria o cartão de cidadão e rege a sua emissão e utilização, primeira alteração à Lei nº37/2014, de 26 de junho, que estabelece um sistema alternativo e voluntário de autenticação dos cidadãos nos portais e sítios na *Internet* da Administração Pública denominado Chave Móvel Digital, e sétima alteração ao Decreto-Lei nº83/2000, de 11 de maio, que aprova o regime legal da concessão e emissão de passaportes;
- Decreto-Lei n.º 10-A/2020 – Estabelece medidas excecionais e temporárias relativas à situação epidemiológica do novo Coronavírus - COVID 19;
- Resolução do Conselho de Ministros nº41/2018 – Define orientações técnicas para a Administração Pública, recomendando-as ao setor empresarial do Estado, em matéria de arquitetura de segurança de redes e sistemas de informação e procedimentos a adotar de modo a cumprir as normas RGPD;
- Lei nº41/2004 de 18 de agosto – Transpõe para a ordem jurídica nacional a Diretiva nº2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas;
- Regulamento (UE) 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 e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados);
- Lei n.º 58/2019 de 8 de agosto – Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento 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 (UE) nº611/2013 da Comissão, de 24 de jungo de 2013, relativo às medidas aplicáveis à notificação da violação de dados pessoais em conformidade com a Diretiva 2002/58/CE;
- Lei nº5/2004 de 10 de fevereiro – Lei das Comunicações Eletrónicas;
- Decisão da Autoridade Nacional de Comunicações (ANCOM), 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 nº109/2009 de 15 de setembro – Aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro nº2005/222/JAI, do Conselho, de 24 de

fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa.

11.1 Resolução de conflitos

Em caso de litígio o titular do certificado pode recorrer a uma Entidade de Resolução Alternativa de Litígios de consumo. A Lista oficial de tais Entidades está disponível no Portal do Consumidor em www.consumidor.gov.pt.

Sem prejuízo da possibilidade de recurso prévio à mediação, caso não seja obtido acordo entre as partes no âmbito de tal procedimento, qualquer uma das partes poderá recorrer à via judicial, ficando desde já fixado como foro competente para o efeito a Comarca de Lisboa.

12 Repositório e auditorias

Toda a informação referente à Entidade de Certificação CMD encontra-se disponível publicamente no repositório SCMD[1].

Todas as intervenções realizadas à Entidade de Certificação CMD são devidamente auditadas por auditores internos. A Entidade de Certificação CMD é auditada por um Organismo de Avaliação da Conformidade (devidamente registado no Organismo Nacional de Acreditação), o qual emite um Relatório de Conformidade (CAR [8]) que é disponibilizado à Entidade Supervisora, para avaliar a continuidade de disponibilização de serviços de confiança, conforme regulamento eIDAS[3].

12.1 Certificações

O prestador qualificado de serviço de confiança (AMA – Agência para a Modernização Administrativa, I.P.) está certificado para a emissão dos certificados qualificados de assinatura eletrónica, conforme regulamento eIDAS[3], podendo tal ser verificado na *eIDAS Trusted List* em em https://webgate.ec.europa.eu/tl-browser/#/tl/PT/8.

[8] *Conformity Assessment Report*

Aprovação

Aprovado pelo Grupo de Gestão.

Assinado por: **ANDRÉ FERREIRA FERRÃO COUTO E VASCONCELOS**

Assinado por: **António Paulo Vicente Simões Maio**
Num. de Identificação: 09777112
Data: 2022.05.11 10:49:43+01'00'