AUTENTICAÇÃO.GOV
CHAVE MÓVEL DIGITAL

Adesão online e por identificação à distância à Chave Móvel digital, e utilização da Chave Móvel Digital e da Assinatura Eletrónica Qualificada via Chave Móvel Digital – Termos e Condições

Procedimento (PR-032)

Nível de Acesso: Público

Versão: 4.0

Data: 16/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

Palavras-chave: SCMD, Serviço Chave Móvel Digital, Procedimento, Termos e Condições, Adesão online e por identificação à distância

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

Histórico de Versões

Versão	Data	Contribuição
1.0	01/Out/2020	Versão aprovada do documento.
2.0	17/Jun/2021	Revisão de documento
3.0	16/Set/2021	Alterações de acordo com o Decreto-Lei n.º 88/2021, assim como relativas à inclusão no SGSI AMA.
4.0	16/Mar/2022	Inclusão da adesão por identificação à distância com recurso a videoconferência.

Anexos e Documentos Relacionados

Documento	Autor	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. 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.
Declaração de Práticas de Operação do SCMD	AMA	Descreve os procedimentos e práticas utilizados pelo SCMD para suportar a sua atividade de assinatura eletrónica qualificada "server-side".
Política CMD de assinatura qualificada	AMA	Política de assinatura qualificada, de acordo com o ETSI TS 119 172 – 1, adaptada ao SCMD.
Declaração de Divulgação de Princípios da EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão	AMA	Resume, de forma simples e acessível, as características descritas na Política de Certificado e Declaração de Práticas de Certificação da EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão.
Declaração de Práticas de Certificação da EC de	AMA	Define os procedimentos e práticas utilizadas pela Entidade de Certificação de Chave Móvel Digital de

Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão		Assinatura Digital Qualificada do Cartão de Cidadão no suporte à sua atividade de certificação digital.
Política de Certificado de Chave Móvel Digital de Assinatura Digital Qualificada	AMA	Apresenta um conjunto de parâmetros que definem o perfil dos Certificados de Assinatura Digital Qualificada emitidos pela Entidade de Certificação de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão.

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 Termos e Condições

A «Chave Móvel Digital» (CMD) é um meio alternativo e voluntário de:

a) Autenticação segura em portais e sítios na Internet;

b) Assinatura eletrónica qualificada, em conformidade com o Regulamento (UE) N.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014.

A todo o cidadão é permitida a associação do seu número de identificação civil a um único número de telemóvel, podendo também associar o seu endereço de correio eletrónico.

No caso de cidadão estrangeiro que não tenha número de identificação civil[1], a associação é efetuada através do número de identificação fiscal constante dos títulos de residência, dos cartões de residência, ou do respetivo número de passaporte.

O sistema é composto por uma palavra-chave permanente, distinta para a autenticação e assinatura, escolhida e alterável pelo utilizador, bem como por um código numérico de utilização única e temporária por cada autenticação ou assinatura.

A CMD gera automaticamente, aquando da introdução da identificação do utilizador e da palavra-chave a ela associada, um código numérico, que é enviado por *Short Message Service* (SMS) para o respetivo número de telemóvel ou, por *push notification* para a aplicação móvel (*app*) Autenticação.Gov (preferencial) registada pelo utilizador.

1.1 Adesão Online à Chave Móvel Digital

A adesão online à Chave Móvel Digital é efetuada através do sítio Autenticação.Gov (https://www.autenticacao.gov.pt/). A validação é efetuada com base no certificado de autenticação do Cartão de Cidadão do requerente, para o que necessitará de ter consigo os seguintes elementos:

- Cartão de Cidadão,
- Código PIN de autenticação, e
- Leitor de cartões.

1.2 Adesão por Biometria à Chave Móvel Digital

É ainda possível através de um serviço, disponibilizado a partir da aplicação Autenticação.gov móvel[2] (*app*), realizar o registo na CMD através da recolha de dados biométricos, utilizando o reconhecimento facial, com deteção de vida como mecanismo de validação da identidade, e também leitura automática dos dados do Cartão de Cidadão, em conformidade com a Lei n.º 37/2014 (com a redação introduzida pelo Decreto-Lei n.º 88/2021).

O processo de registo na CMD através da *app* Autenticação.gov recorre à identificação à distância do cidadão com base na combinação da verificação de diferentes fatores de autenticação, em conformidade com o Despacho n.º 2705/2021 do Gabinete Nacional de

[1] A adesão à CMD online e por identificação à distância é apenas permitida a cidadãos nacionais, portadores de Cartão de Cidadão válido.

[2] https://www.autenticacao.gov.pt/web/guest/aplicacao/autenticacao-gov-movel

Segurança para os efeitos definidos na alínea d) do n.º 1 do artigo 24.º do Regulamento (UE) N.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, nomeadamente:

- Verificação que é a pessoa titular do documento de identificação que está, em tempo real, a efetuar o pedido de registo CMD, através de tecnologia de "deteção de vida" (*liveness detection*);
- Verificação que o documento de identificação apresentado é autêntico e corresponde à pessoa que está a efetuar o pedido de registo CMD, com recurso a tecnologia de inteligência artificial e de *deep learning*;
- Verificação da comparação biométrica facial com base nos dados biométricos do cidadão que está a efetuar o pedido de registo CMD, recolhidos presencialmente pela autoridade nacional responsável pela emissão do documento de identificação, no momento da sua emissão;
- Verificação que o cidadão que está a efetuar o pedido de registo CMD tem acesso ao número de telemóvel indicado no processo;
- Verificação da comparação de dados recolhidos presencialmente pela autoridade nacional responsável pela emissão do documento de identificação, no momento da sua emissão.

1.3 Adesão por Videoconferência à Chave Móvel Digital

O registo na CMD pode ainda ser efetuado por identificação à distância com recurso a videoconferência, através de um dispositivo com *browser web* e câmara, Este processo é conduzido pelo operador de videoconferência, com o auxílio de ferramentas automáticas de reconhecimento facial e de leitura automática dos dados do Cartão de Cidadão, para validação da identidade do requerente, em conformidade com a Lei n.º 37/2014 (com a redação introduzida pelo Decreto-Lei n.º 88/2021).

O processo de registo na CMD por identificação à distância com recurso a videoconferência, recorre à combinação da verificação de diferentes fatores de autenticação, em conformidade com o Despacho n.º 154/2017 do Gabinete Nacional de Segurança para os efeitos definidos na alínea d) do n.º 1 do artigo 24.º do Regulamento (UE) N.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, nomeadamente:

- Verificação que é a pessoa titular do documento de identificação que está, em tempo real e sem interrupções/pausas, a requerer o pedido de registo CMD;
- Verificação que o documento de identificação apresentado é autêntico e corresponde ao requerente;
- Verificação da comparação biométrica facial com base nos dados biométricos do requerente, recolhidos presencialmente pela autoridade nacional responsável pela emissão do documento de identificação, no momento da sua emissão;
- Verificação que o requerente tem acesso ao número de telemóvel indicado no processo;
- Verificação da comparação de dados recolhidos presencialmente pela autoridade nacional responsável pela emissão do documento de identificação, no momento da sua emissão.

Para adesão por videoconferência à Chave Móvel Digital, necessitará de ter consigo os seguintes elementos:

- Cartão de Cidadão,

- Telemóvel, e
- (opcional) Endereço de correio eletrónico.

O processo de registo pode ser cancelado em qualquer altura da sessão de videoconferência, por iniciativa do operador ou do requerente. Em especial, qualquer uma das seguintes situações é motivo suficiente para o operador cancelar a sessão, de acordo com o Despacho n.º 154/2017 do Gabinete Nacional de Segurança:

- A sessão de videoconferência não ser realizada em tempo real e sem interrupções/pausas.
- O requerente não ter consigo o documento de identificação permitido ou o telemóvel, levando a interrupção/pausa na sessão ou a pedido a pessoa externa à sessão.
- O cidadão que agendou a sessão não ser o requerente que está a ser identificado.
- A qualidade da comunicação não ser adequada para permitir a identificação clara dos elementos e características de segurança do documento de identificação.
- Existir suspeita na autenticação do requerente.
- Caso não se verifiquem as condições técnicas necessárias à boa condução do processo de comprovação da identificação, nomeadamente: nos casos de existência de fraca qualidade de imagem, de condições deficientes de luminosidade ou som, ou de interrupções na transmissão do vídeo.
- Caso o documento de identificação apresentado durante a videoconferência ofereça dúvidas quanto ao seu teor, autenticidade, atualidade, exatidão ou suficiência.
- Caso existam suspeitas quanto à veracidade dos elementos de identificação.
- Caso não seja possível validar o documento de identificação, com recurso às ferramentas automáticas utilizadas.
- Caso não seja possível comprovar que o requerente tem acesso ao número de telemóvel indicado no processo.

1.4 Autenticação e a Assinatura Eletrónica Qualificada via Chave Móvel Digital

Após adesão à CMD pode utilizar os serviços de autenticação e assinatura eletrónica qualificada. São serviços geridos pela Agência para a Modernização Administrativa, I.P., adiante abreviadamente designada por "AMA".

Antes de aceder e aceitar expressamente utilizar estes serviços, deve ler atentamente os seus Termos e Condições.

Quaisquer tentativas de alterar a informação, ou qualquer outra ação que possa causar dano e pôr em risco a integridade do sistema, são estritamente proibidas de acordo com a legislação em vigor.

É proibida a utilização de conteúdos disponibilizados pela AMA para fins ilegais ou quaisquer outros fins que possam ser considerados indignos ou abusivos. Proíbe-se ainda a criação ou introdução de qualquer tipo de vírus ou outro código ou programa que contenham propriedades destrutivas ou prejudiciais ao seu funcionamento.

O utilizador da app Autenticação.gov e do sítio Autenticação.gov obriga-se a cumprir escrupulosamente a legislação aplicável, nomeadamente, em matéria de criminalidade informática e de direitos de propriedade intelectual, sendo exclusivamente responsável pela infração destes normativos.

Todos os conteúdos, incluindo eventuais vídeos, gráficos, textos, imagens, desenhos, músicas ou sons e quaisquer outras informações são propriedade da AMA, ou foram incluídos com permissão das entidades que legitimamente detêm os direitos de autor sobre os mesmos.

A proteção dos direitos de autor e de propriedade industrial sobre os conteúdos presentes na app e no sitio estende-se a todas as cópias de parte ou da totalidade da informação contida no mesmo.

1.5 Privacidade

A AMA respeita o seu direito à privacidade e não recolhe qualquer informação pessoal sobre si sem o seu consentimento. Os meios de acesso, informação, retificação, portabilidade, revogação e apagamento dos seus dados são disponibilizados através da sua conta no sítio Autenticação.Gov.

Para a utilização do serviço de adesão à CMD por identificação à distância e online, será necessário recolher os seus dados pessoais, para as finalidades indicadas, conforme se discrimina em seguida:

Dados pessoais recolhidos	**Adesão por biometria**	**Adesão por vídeoc.**	**Adesão online**
Fotografia da frente e verso do Cartão de Cidadão e dos dados nele constantes	X	X	
Fotografia do rosto e respetivo *template* biométrico	X	X	
Número de Telemóvel	X	X	X
Fingerprint do dispositivo	X		
Endereço de Correio Eletrónico (opcional)	X	X	X
Representação criptográfica da Palavra-Chave de autenticação	X	X	X
Representação criptográfica da Palavra-chave de assinatura	X	X	X
Dados recolhidos aquando do pedido do Cartão de Cidadão (Código Postal, fotografia, Número de Identificação Civil, data de nascimento, data de expiração, nome, apelido, sexo, nacionalidade, nome do pai e nome da mãe)	X	X	X
Vídeo de todo o processo de registo/adesão		X	

No âmbito destes serviços os dados recolhidos são conservados pelos prazos indicados em seguida:

a) A fotografia do rosto e respetivo *template* biométrico, e os dados nele constantes, são eliminados em processo diário, após conclusão do processo de adesão, conforme ponto 5.3.1.2 do Despacho n.º 2705/2021 do Gabinete Nacional de Segurança;

b) A fotografia da frente e verso do Cartão de Cidadão é eliminada no prazo de 10 dias, conforme ponto 19 do artigo 2º da Lei n.º 37/2014 (com a redação introduzida pelo Decreto-Lei n.º 88/2021) e, ponto 5.3.1.3 do Despacho n.º 2705/2021 do Gabinete Nacional de Segurança;

c) Os dados recolhidos aquando do pedido do Cartão de Cidadão são apenas utilizados para validação dos documentos apresentados no registo, sendo eliminados imediatamente (à exceção dos dados necessário para o registo, indicados na alínea seguinte);

d) Os dados relativos ao registo de atribuição da CMD (Nome, Apelido, data de nascimento, data de expiração do CC, Número de Telemóvel, *fingerprint* do dispositivo, Endereço de Correio Eletrónico, representação criptográfica da Palavra-Chave de autenticação, representação criptográfica da Palavra-chave de assinatura) são conservados 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;

e) O vídeo de todo o processo de registo/adesão é mantido conservado durante sete anos após o fim da validade do respetivo certificado (no caso de registo/adesão com sucesso), de acordo com o ponto 11 do anexo A do Despacho n.º 154/2017 do Gabinete Nacional de Segurança e, a alínea f) do artigo 13º do Decreto-Lei nº 12/2021;

f) No caso de adesão por videoconferência, o vídeo de todo o processo de registo/adesão é conservado por um período máximo de 3 anos, para garantia da qualidade de serviço e ao abrigo da responsabilidade extracontratual do Estado (conforme artigo 5º da Lei n.º 67/2007, de 31 de Dezembro, determinado conforme o Artº 498 do Código Civil).

Os utilizadores da CMD podem monitorizar o seu histórico de autenticações e assinaturas no sítio Autenticação.gov. Para a utilização dos serviços de autenticação e assinatura eletrónica qualificada, será necessário recolher os seus dados pessoais, para as finalidades indicadas, conforme se discrimina em seguida:

Dados pessoais recolhidos	**Autenticação**	**Assinatura Qualificada**
Nome	X	
Número de Telemóvel	X	X
Número de Identificação Civil	X	X
Nome do Ficheiro a assinar		X
Identificador do Ficheiro a assinar		X
Representação criptográfica (*hash*) do ficheiro a assinar		X
Certificado qualificado do cidadão		X

No âmbito destes serviços os dados recolhidos são conservados pelos prazos indicados em seguida:

a) Os dados pessoais recolhidos para a autenticação através da CMD são eliminados no prazo de um ano após a respetiva ocorrência.

b) Os dados pessoais recolhidos para a assinatura efetuada através da CMD são conservados 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.

O utilizador pode, a todo o tempo, alterar a sua palavra-passe permanente no sítio na Autenticação.gov.

Por questões de segurança pode ser solicitada ao utilizador a alteração da sua palavra-chave.

O utilizador pode também proceder à alteração do seu número de telefone e ou endereço de correio eletrónico. A alteração do número de telefone corresponde à desativação da CMD associada a um número de telefone, seguida da adesão à CMD com associação a um novo número de telefone.

Por motivos de segurança a palavra-passe permanente pode ser bloqueada após a subsequente introdução de códigos alfanuméricos errados. O desbloqueio é efetuado nos termos previstos para o registo presencial ou eletrónico. Quando se verifique a utilização abusiva pode haver lugar à sua suspensão temporária por períodos de 24 horas.

Pode ser feito o cancelamento quando exista conhecimento que o documento de registo tenha sido cancelado por motivos associados à fraude de identidade.

A CMD e o certificado eletrónico de assinatura da CMD são cancelados:

a) Nos casos de morte do titular ou da sua incapacidade superveniente, através de informação enviada pelo Instituto dos Registos e do Notariado, I. P.;

b) No caso do documento de identificação perder a validade.

Adicionalmente, o certificado eletrónico de assinatura da CMD é cancelado nos casos de motivos para revogação identificados na "Declaração de Práticas de Certificação da EC de Chave Móvel Digital de Assinatura Qualificada do Cartão de Cidadão[3]".

O utilizador pode solicitar, a todo o tempo, a revogação da CMD ou da assinatura qualificada, implicando o respetivo cancelamento, no sítio Autenticação.gov.

Os dados pessoais recolhidos não são partilhados sem que seja solicitado previamente o seu consentimento.

Encontram-se implementadas as medidas de segurança sobre o tratamento indicadas em seguida:

- Para o serviço de adesão por biometria, todas as medidas previstas no Despacho n.º 2705/2021 do Gabinete Nacional de Segurança;
- Para o serviço de adesão por biometria e para o serviço de adesão online, todas as medidas previstas no Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho;
- Para a utilização da CMD (autenticação e assinatura) são seguidas as recomendações obrigatórias previstas na RCM 41/2018 que são aplicáveis.

A arquitetura destes sistemas assegura que toda e qualquer informação é recolhida apenas com o consentimento do cidadão para a finalidade a que foi dado o consentimento, sendo apenas a informação de registo e dos *logs* aplicacionais armazenada nos sistemas da AMA. Todas as restantes informações solicitadas aos utilizadores pelos serviços e organismos da Administração Pública ou entidades privadas é apenas guardada nos sistemas de informação desses serviços e organismos ou dessas entidades.

1.6 Exoneração de responsabilidade

A AMA não poderá ser responsabilizada por quaisquer prejuízos ou danos em sede de responsabilidade civil (incluindo, mas sem que a estes estejam limitados, danos emergentes, lucros cessantes e danos morais, causados direta ou indiretamente), que surjam em

[3] https://pki.cartaodecidadao.pt/publico/politicas/PJ.CMDA_33_signed.pdf

consequência da utilização, correta ou incorreta deste serviço e dos seus conteúdos pelo utilizador ou do acesso ao computador e sistema informático do utilizador por terceiros.

O utilizador é responsável pela guarda e correta utilização da sua informação pessoal, bem como responsável por qualquer dano ou prejuízo causado à AMA ou a terceiros, resultante da utilização incorreta, perda ou furto da informação pessoal. Os utilizadores são responsáveis pela utilização segura da sua palavra-chave, bem como do telemóvel e endereço de correio eletrónico associados.

A presente informação deve ser encarada na sua vertente informativa. Apesar dos esforços da AMA em manter os conteúdos atualizados e fidedignos, estes podem conter incorreções, erros de escrita ou estar desatualizados, pelo que não poderá a AMA ser responsabilizada no que respeita à completa exatidão e atualidade de qualquer informação.

O presente serviço contem ligações para serviços operados por entidades terceiras sobre os quais não tem controlo e pelos quais não assume qualquer responsabilidade.

A leitura dos presentes termos e condições não dispensa a consulta das normas legais em vigor, aprovadas oficialmente, publicadas nas edições e suportes originais (nomeadamente o Diário da República ou o Jornal Oficial da União Europeia).

1.7 Legislação e Regulamentação aplicável

- Lei n.º 37/2014, de 26 de junho, alterada pela Lei n.º 32/2017, de 1 de junho, pelo artigo 331.º da Lei n.º 71/2018, de 31 de dezembro, e pelo Decreto-Lei n.º 88/2021 de 3 de novembro.
- Portaria n.º 77/2018, de 16 de março, alterada pela Portaria n.º 190-A/2019, de 21 de junho.
- 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 (RGPD).
- Lei n.º 58/2019, de 8 de agosto, que assegura a execução, na ordem jurídica nacional, do RGPD.
- Resolução do Conselho de Ministros n.º 41/2018.
- Regulamento (UE) 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.
- Despacho n.º 2705/2021 do Gabinete Nacional de Segurança ("Identificação de pessoas físicas através de procedimentos de identificação à distância com recurso a sistemas biométricos automáticos de reconhecimento facial").
- Despacho n.º 154/2017 do Gabinete Nacional de Segurança ("Identificação de pessoas físicas através de procedimentos de identificação à distância com recurso a videoconferência").

1.8 Lei aplicável e foro competente

Os presentes Termos e Condições são regidos e interpretados de acordo com a lei portuguesa.

É competente o Tribunal da área territorial de Lisboa com exclusão de qualquer outro para dirimir quaisquer conflitos que resultem da interpretação e aplicação dos presentes Termos e Condições para a utilização deste serviço.

Aprovação

Aprovado pelo Grupo de Trabalho de Gestão.

Assinado por: **ANDRÉ FERREIRA FERRÃO COUTO E VASCONCELOS**
Data: 2022.08.24 21:07:29+01'00'