

DIGITALSIGN - CERTIFICADORA DIGITAL, SA.

A CARTEIRA EUROPEIA DE IDENTIDADE DIGITAL O QUE MUDA PARA AS ORGANIZAÇÕES

CONTEXTO, CASOS DE USO E O PAPEL DOS PRESTADORES QUALIFICADOS DE SERVIÇOS DE CONFIANÇA

ÍNDICE

1.	O que é a Carteira Europeia de Identidade Digital	3
2.	A arquitetura de confiança	4
3.	Quem emite a Carteira, e porque isso importa	4
4.	Cronologia	4
5.	O que muda para os cidadãos	5
6.	O que muda para as organizações	5
7.	Casos de uso: onde a Carteira cria valor	6
7.1.	Serviços financeiros, o foco imediato	6
7.2.	Outros setores de elevado valor	6
8.	O papel dos PQSC, e da DigitalSign, nesta transição	7
9.	A convergência com o novo Regulamento Anti-Branqueamento de Capitais	7
10.	Conclusão	8

SUMÁRIO EXECUTIVO

A forma como provamos quem somos está prestes a mudar. Durante décadas, a identificação digital assentou em sistemas nacionais fragmentados, em processos manuais e na digitalização de documentos físicos. Com o Regulamento (UE) 2024/1183, o eIDAS 2.0, que instituiu o Regime Europeu para a Identidade Digital, a União Europeia estabelece um novo padrão: a Carteira Europeia de Identidade Digital.

Cada Estado-Membro fica obrigado a disponibilizar pelo menos uma Carteira certificada no prazo de 24 meses a contar da entrada em vigor dos respetivos atos de execução, ou seja, previsivelmente até ao final de 2026. E, o mais tardar 36 meses após esses atos, portanto até cerca de 24 de dezembro de 2027, as organizações de setores regulados passam a estar obrigadas a aceitar a Carteira como meio de identificação, a pedido do respetivo titular, nos termos do artigo 5.º-F do eIDAS 2.0.

No presente *white paper*, explicamos em que consiste a Carteira Europeia de Identidade Digital, qual o seu papel na transformação digital dos cidadãos e, sobretudo, das organizações, e apresentamos os principais casos de uso, com destaque natural para o setor financeiro sem esquecer outros domínios de elevado valor. A Carteira Europeia de Identidade Digital não dispensa os Prestadores Qualificados de Serviços de Confiança (PQSC): pelo contrário, industrializa a procura por aquilo que um PQSC está habilitado a fazer, isto é, comprovar identidades, certificar atributos e assinar ou selar com valor jurídico.

1. O QUE É A CARTEIRA EUROPEIA DE IDENTIDADE DIGITAL

A Carteira Europeia de Identidade Digital é, na definição do artigo 3.º, ponto 42), do eIDAS 2.0, um meio de identificação eletrónica que permite ao seu titular armazenar, gerir e validar de forma segura os seus dados de identificação pessoal e certificados eletrónicos de atributos, fornecê-los a quem deles necessite e, ainda, assinar com assinatura eletrónica qualificada e apor selos eletrónicos qualificados.

Por palavras simples, trata-se de uma aplicação móvel na qual o cidadão, o residente ou a empresa passa a deter, num único lugar e sob o seu controlo, a sua identidade digital e um conjunto de atributos verificados: habilitações académicas, certificações profissionais, licenças, mandatos de representação, entre muitos outros.

Um princípio distingue a Carteira Europeia de Identidade Digital dos sistemas de identificação atuais: a divulgação seletiva de atributos, expressamente consagrada no artigo 5.º-A, n.º 4, alínea a). O titular partilha apenas a informação estritamente necessária a cada interação. Deste modo, para comprovar a maioridade, não tem de revelar a data de nascimento; para provar uma qualificação profissional, não tem de expor o documento de identidade completo. Ora, o controlo dos dados permanece, em permanência com o titular.

A base jurídica é o Regulamento (UE) 2024/1183, que alterou o Regulamento (UE) n.º 910/2014 e entrou em vigor em maio de 2024.

DIVULGAÇÃO SELETIVA

Com a Carteira Europeia de Identidade Digital, provar um facto deixa de obrigar a revelar um documento inteiro. O titular partilha apenas o atributo estritamente necessário, por exemplo «maior de 18 anos», sem expor a data de nascimento nem a identidade completa. É um ganho simultâneo de conveniência e de privacidade.

2. A ARQUITETURA DE CONFIANÇA

Três elementos sustentam a confiança na Carteira Europeia de Identidade Digital, e importa distingui-los: i) os *Dados de Identificação Pessoal* (PID, na sigla inglesa), definidos no artigo 3.º, ponto 3), que permitem determinar a identidade do titular e constituem o núcleo identitário da Carteira; ii) os *certificados eletrónicos de atributos*, que atestam factos específicos sobre o titular, como uma morada, um número de identificação fiscal, uma habilitação ou um mandato, e que, quando emitidos por um PQSC e cumpridos os requisitos do anexo V do Regulamento, assumem a forma de certificado eletrónico qualificado de atributos (QEAA), definido no artigo 3.º, ponto 45); iii) a *assinatura eletrónica qualificada* e o *selo eletrónico qualificado*, que a Carteira integra nativamente e que conferem, respetivamente à pessoa singular e à pessoa coletiva, a possibilidade de assinar e de selar documentos com pleno valor jurídico.

Quanto ao rigor da identificação, o eIDAS define três níveis de garantia, reduzido, substancial e elevado (artigo 8.º), que exprimem a força probatória de um meio de identificação eletrónica. Cumpre sublinhar que a Carteira é fornecida, por imposição do artigo 5.º-A, n.º 11, ao abrigo de um sistema de identificação eletrónica com nível de garantia elevado, o mais exigente. Importa, ainda assim, não confundir planos: o nível de garantia respeita ao meio de identificação; os certificados de atributos, por seu turno, são serviços de confiança e retiram o seu valor jurídico do estatuto qualificado, e não de uma graduação por níveis de garantia.

3. QUEM EMITE A CARTEIRA, E PORQUE ISSO IMPORTA

A Carteira pode ser fornecida pelo próprio Estado-Membro, por entidade por este mandatada ou mediante o reconhecimento de uma solução privada. Ademais, o Regulamento prevê que os Dados de Identificação Pessoal sejam emitidos por uma autoridade pública ou por quem esta delegue, o que abre a porta a que um PQSC devidamente certificado atue nesse papel.

Esta distinção é relevante. Um PQSC privado, tal como a DigitalSign, opera sob supervisão regulatória europeia, com deveres restritos de segurança, auditabilidade e proteção de dados, mas com a agilidade, a capacidade de inovação e a proximidade ao mercado que uma entidade pública raramente consegue assegurar. É esta combinação que torna os PQSC atores centrais na implementação da Carteira, não apenas como integradores, mas como emissores de confiança qualificada.

A confiança de todo o sistema é, por fim, sinalizada por uma marca própria: o artigo 3.º, ponto 50), institui a «Marca de confiança 'UE' para a carteira de identidade digital», indicação verificável e reconhecível de que uma dada Carteira foi fornecida em conformidade com o Regulamento.

4. CRONOLOGIA

Momento	Marco
Maio de 2024	Entrada em vigor do eIDAS 2.0, o Regulamento (UE) 2024/1183.
Até cerca de 24 dez. 2026	Cada Estado-Membro disponibiliza pelo menos uma Carteira certificada, no prazo de 24 meses após os atos de execução (art. 5.º-A, n.º 1).
10 jul. 2027	O Regulamento Anti-Branqueamento de Capitais (AMLR) torna-se aplicável.

Até cerca de 24 dez. 2027	As organizações de setores regulados passam a ser obrigadas a aceitar a Carteira, a pedido do titular, no prazo de 36 meses após os atos de execução (art. 5.º-F, n.º 2).
---------------------------	---

Os prazos de 24 e 36 meses contam-se, nos termos do Regulamento, da entrada em vigor dos atos de execução pertinentes; as datas indicadas resultam desse cálculo, pressupondo a sua entrada em vigor em 24 de dezembro de 2024.

5. O QUE MUDA PARA OS CIDADÃOS

Para o cidadão, a Carteira Europeia de Identidade Digital representa conveniência com controlo. Uma única aplicação passa a permitir identificar-se junto de serviços públicos e privados, em qualquer Estado-Membro, assinar contratos com valor jurídico, aceder a serviços de saúde ou comprovar qualificações, revelando de cada vez apenas o estritamente necessário. A divulgação seletiva devolve ao titular o domínio sobre os seus dados, invertendo a lógica atual, em que provar um facto simples obriga, as mais das vezes, a expor um documento inteiro.

6. O QUE MUDA PARA AS ORGANIZAÇÕES

É aqui que reside o essencial. A partir do prazo do artigo 5.º-F, n.º 2, as organizações que estejam obrigadas, por força da lei ou de contrato, a utilizar autenticação forte do utilizador, categoria em que se incluem, designadamente, a banca, os serviços financeiros, os seguros, as telecomunicações, a energia, os prestadores de serviços de criptoativos e as plataformas em linha de muito grande dimensão, passam a ter de aceitar a Carteira Europeia de Identidade Digital como meio de identificação, a pedido do titular.

Cumpr, a este respeito, uma nota terminológica: o Regulamento chama «utilizador» à organização que aceita a Carteira Europeia de Identidade Digital e nela confia, reservando o termo «utente» para o titular. Para clareza, usamos aqui «organização» e «titular».

OBRIGAÇÃO DE ACEITAÇÃO (ART. 5.º-F DO EIDAS 2.0)

A aceitação da Carteira não é uma opção comercial, é uma obrigação legal para as organizações de setores regulados sujeitas a autenticação forte do utilizador, a cumprir a pedido do titular, no prazo de 36 meses a contar da entrada em vigor dos atos de execução, previsivelmente até 24 de dezembro de 2027.

Não obstante, as implicações vão muito além do mero cumprimento:

- *Onboarding* mais rápido e menos oneroso. A identidade do cliente já foi verificada e certificada na origem. A organização recebe os atributos de que necessita de forma instantânea, sem recolha manual de documentos nem verificações redundantes, reduzindo o tempo de integração e os custos operacionais.
- Operação verdadeiramente pan-europeia. Uma identidade verificada num Estado-Membro é reconhecida em todos os outros. Elimina-se um dos maiores pontos de fricção, a reavaliação de identidade em cada novo mercado, e uma única integração passa a servir os 27 mercados.
- Contratos com pleno valor jurídico à distância. A Carteira Europeia de Identidade Digital integra nativamente a assinatura eletrónica qualificada, que tem o mesmo valor jurídico

que a assinatura manuscrita em toda a União. Celebrar contratos à distância, de forma segura e sem papel, deixa de ser exceção para passar a norma.

- Menos dados, menos risco. A divulgação seletiva significa que a organização recolhe apenas o estritamente necessário a cada transação. Menos dados armazenados implicam menor exposição em caso de incidente de segurança e menor esforço de cumprimento do RGPD, desde logo por via da minimização dos dados.

7. CASOS DE USO: ONDE A CARTEIRA CRIA VALOR

7.1. SERVIÇOS FINANCEIROS, O FOCO IMEDIATO

O setor financeiro é, a um tempo, o de maior maturidade e o de procura legalmente garantida, porquanto é aí que a obrigação de aceitação do artigo 5.º-F se cruza com os deveres de verificação de identidade. Destacam-se os seguintes casos:

- Abertura de conta e *onboarding* (KYC): o cliente apresenta os seus Dados de Identificação Pessoal e os certificados de atributos exigidos, com divulgação seletiva, reduzindo o processo de dias a minutos.
- Diligência devida (CDD) em matéria de branqueamento de capitais: como desenvolvemos adiante, o AMLR reconhece expressamente a Carteira e os certificados qualificados de atributos como meios idóneos de verificação.
- Autenticação forte do cliente (SCA): a Carteira suporta nativamente a autenticação forte alinhada com a DSP2, e o artigo 5.º-F obriga a banca e os prestadores de serviços de pagamento a aceitá-la, a pedido do cliente.
- Assinatura qualificada de contratos de crédito, mútuo, seguro ou investimento: identificado o cliente através da Carteira, a contratação encerra-se integralmente à distância, com assinatura eletrónica qualificada.
- Prestadores de serviços de criptoativos (MiCA): também estes figuram entre os obrigados a aceitar a Carteira, o que padroniza e reaproveita a verificação de identidade.

7.2. OUTROS SETORES DE ELEVADO VALOR

- Saúde: receita eletrónica e resumo clínico transfronteiriços, com apresentação de credenciais de profissional de saúde e de direitos de comparticipação.
- Educação e qualificações profissionais: diplomas, microcredenciais e licenças profissionais como credenciais verificáveis, com verificação instantânea e à prova de fraude por empregadores e reguladores.
- Mobilidade e viagens: carta de condução em formato digital (mDL), credenciais de viagem e *check-in* simplificado.
- Telecomunicações: registo e ativação de cartões SIM com verificação de identidade, num setor igualmente abrangido pela obrigação de aceitação.
- Setor público: identificação e autenticação junto de serviços nacionais e transfronteiriços, articulando-se, em Portugal, com a Chave Móvel Digital e a aplicação gov.pt.

- Verificação de idade: prova criptográfica de maioridade sem revelar a data de nascimento nem a identidade, resposta direta aos deveres de proteção de menores decorrentes do Regulamento dos Serviços Digitais.
- Relações entre empresas (B2B): comprovação imediata de poderes de representação, do número de identificação de pessoa coletiva e de mandatos, com relevância para a contratação pública, a faturação eletrónica e a contratação entre empresas.

EVIDÊNCIA DE MATURIDADE: OS PROJETOS-PILOTO DE LARGA ESCALA

A Carteira Europeia de Identidade Digital não é um exercício teórico. Quatro consórcios europeus de larga escala testaram-na, com centenas de entidades públicas e privadas: POTENTIAL (serviços públicos, abertura de conta bancária, registo de SIM, carta de condução, assinatura qualificada e receita eletrónica), EWC (credenciais de viagem, pagamentos e carteira empresarial), NOBID (pagamentos) e DC4EU (educação e segurança social).

8. O PAPEL DOS PQSC, E DA DIGITALSIGN, NESTA TRANSIÇÃO

A Carteira multiplica, não elimina, a procura por serviços de confiança qualificados. Um PQSC como a DigitalSign intervém, em concreto, em quatro frentes:

- emissão de certificados eletrónicos qualificados de atributos (QEAA), com valor jurídico em toda a União Europeia;
- assinaturas eletrónicas qualificadas e selos eletrónicos qualificados, o produto regulado por excelência, agora consumível a partir da Carteira Europeia de Identidade Digital;
- identificação à distância de pessoas, com base na norma ETSI TS 119 461, para a integração de titulares e a emissão de credenciais ao nível de garantia elevado;
- integração e verificação para as organizações que aceitam a Carteira Europeia de Identidade Digital, isto é, uma única via para aceitar, com segurança, qualquer Carteira europeia;

A DigitalSign é um Prestador Qualificado de Serviços de Confiança, supervisionado pelo Gabinete Nacional de Segurança e reconhecido ao nível europeu. Com mais de duas décadas de experiência em identidade digital e serviços de confiança, encontra-se posicionada para acompanhar organizações e cidadãos em todas as dimensões desta transição, da emissão de credenciais qualificadas à integração nos processos de negócio.

9. A CONVERGÊNCIA COM O NOVO REGULAMENTO ANTI-BRANQUEAMENTO DE CAPITALS

Em 10 de julho de 2027, o Regulamento (UE) 2024/1624, o AMLR, torna-se aplicável, harmonizando os deveres de diligência quanto à clientela em toda a União. A Carteira e o AMLR funcionam em conjunto: a Carteira fornece o meio de verificação; o AMLR define o grau de rigor exigido. Com efeito, o artigo 22.º, n.º 6, alínea b), do AMLR reconhece os meios de identificação eletrónica de nível substancial ou elevado e os serviços de confiança qualificados como métodos idóneos de verificação de identidade à distância. E o próprio eIDAS 2.0, no considerando 62, aponta a identificação eletrónica segura e o fornecimento de certificados de atributos como

solução para o setor dos serviços financeiros cumprir a diligência quanto à clientela. O mesmo processo que melhora a experiência do cliente cumpre, assim, a regulação.

10. CONCLUSÃO

A Carteira Europeia de Identidade Digital não é apenas uma mudança tecnológica. É a construção de uma infraestrutura europeia de confiança que redefine a relação das organizações com os seus clientes, colaboradores e parceiros. Para quem a encarar como oportunidade, e não apenas como obrigação, traz processos mais eficientes, alcance verdadeiramente europeu e uma base de confiança digital com valor económico mensurável.

Para as organizações que querem estar preparadas em 2027, o momento de começar é agora.

Quer saber como a DigitalSign pode apoiar a sua organização na transição para o eIDAS 2.0? Fale com a nossa equipa.