PARECER DA EBA SOBRE OS ELEMENTOS DE AUTENTICAÇÃO FORTE DO CLIENTE DE ACORDO COM A DSP2

Julho de 2019

Introdução

No dia 21 de Junho foi publicado o Parecer da Autoridade Bancária Europeia (EBA, na sigla inglesa) sobre os elementos de autenticação forte do cliente de acordo com a Directiva 2015/2366 ("DSP2").

Este parecer da EBA (EBA-Op-2019-06), sendo dirigido às autoridades competentes nacionais, contém informação muito relevante para os utilizadores e para os prestadores de serviços de pagamentos.

A partir de 14 de Setembro de 2019[1] os prestadores de serviços de pagamento são obrigados a aplicar a autenticação forte do cliente sempre que este aceda online à sua conta de pagamento, inicie uma operação de pagamento electrónico ou realize uma acção, através de um canal remoto, que possa envolver risco de fraude no pagamento ou de outros abusos.

Nos termos da DSP2[2] , «autenticação forte do cliente» consiste numa autenticação baseada na utilização de dois ou mais elementos do cliente pertencentes às categorias "conhecimento" (algo que só o utilizador conhece), "posse" (algo que só o utilizador possui) e "inerência" (algo que o utilizador é), os quais são independentes, na medida em que a violação de um deles não compromete a fiabilidade dos outros, e que é

[1] Data em que entra em vigor o Regulamento Delegado (UE) 2018/389 da Comissão, de 27 de Novembro de 2017, que complementa a DSP2.

[2] E do Decreto-Lei n.º 91/2018, de 12 de Novembro, que transpõe a DSP2 para o ordenamento jurídico português

concebida de modo a proteger a confidencialidade dos dados de autenticação.

Neste Parecer a EBA identifica, embora não exaustivamente, os elementos que podem ser considerados em cada uma das três categorias previstas no âmbito da autenticação forte do cliente ("conhecimento", "posse" e "inerência"), dos quais se salientam, a título exemplificativo, os seguintes:

Elementos de "conhecimento"

A EBA admite como elementos de conhecimento a utilização de palavras-passe, PIN's, respostas a uma perguntas baseadas em informações conhecidas pelo utilizador ou, ainda, o desenho de padrões de desbloqueio em monitores tácteis.

Esclarece, todavia, que as informações impressas nos cartões de pagamento não constituem elementos de conhecimento e que um cartão com códigos de segurança dinâmicos pode ser considerado um elemento de posse mas não um elemento de conhecimento. Clarifica, ainda, que o nome de utilizador e o endereço de correio electrónico não podem ser considerados elementos de conhecimento.

Elementos de "posse"

Segundo a EBA, um dispositivo pode ser utilizado como elemento de posse desde que conjugado com um "meio confiável para confirmar a posse através da geração ou recepção de um elemento de validação dinâmica no dispositivo", concretizável através da geração de uma palavra-passe de utilização única, gerada por software ou hardware, tal como um token ou uma SMS. Neste último caso, o elemento de posse não é a própria SMS, mas o cartão SIM associado ao número de telemóvel.

A posse poderá também ser demonstrável através de uma assinatura digital, gerada com a utilização de uma chave privada, ou ainda através de um "QR Code" inserido num cartão e reconhecido por um dispositivo de leitura.

Elementos de "inerência"

Clarifica-se que a categoria "inerência" poderá incluir dados biométricos, tanto biológicos como comportamentais, relacionados com características físicas ou psicológicas (e respectivos processos comportamentais gerados), que identifiquem o utilizador especificamente autorizado. Sublinha-se, contudo, que a aceitação de qualquer elemento de "inerência" à luz da DSP2, dependerá da qualidade da sua implementação concreta.

A categoria "inerência" poderá incluir, segundo o parecer da EBA, o reconhecimento óptico da retina e íris, impressão digital, voz, veias, mãos ou face, mas também o reconhecimento de padrões de escrita, do ângulo em que o utilizador segura o aparelho de comunicação que utiliza ou o ritmo cardíaco do utilizador, desde que a medida implementada implique uma "probabilidade muito baixa de um utilizador não autorizado se autenticar como o pagador [legítimo]"

Possível período de adaptação

A EBA esclarece que as autoridades competentes nacionais poderão facultar um período de tempo adicional para a adopção de soluções compatíveis com mecanismos de autenticação forte, desde que os prestadores de serviços de pagamento tenham estabelecido um plano de migração para esses novos mecanismos, acordado esse plano com as autoridades competentes nacionais e o cumpram de forma expedita.