S€PA.PT

Newsletter • N.º 15 • maio 2019

BANCO DE PORTUGAL
EUROSISTEMA

Editorial

Ao longo dos últimos meses, o mercado de pagamentos de retalho tem sido fortemente influenciado pelas adaptações resultantes da entrada em vigor da Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho, relativa aos serviços de pagamento no mercado interno (DSP2). Conforme se antevia, as implicações trazidas pela DSP2 e, no caso português, pelo Decreto-Lei n.º 91/2018, de 12 de novembro, que veio criar no ordenamento jurídico interno o novo Regime Jurídico dos Serviços de Pagamento e Moeda Eletrónica, são substanciais e vieram criar condições para o posicionamento de novos intervenientes, por um lado, e da prestação de novos tipos de serviços, por outro.

Entre as alterações de maior significado encontra-se a necessidade de adotar novas práticas de autenticação forte dos clientes quando estejam em causa acessos *online* a contas de pagamento, bem como a iniciação de pagamentos eletrónicos (presenciais ou remotos). Aqui, será consubstanciado um novo paradigma, que reforçará a segurança tanto para os clientes (ordenante e beneficiário) como para os prestadores de serviços de pagamento. A adoção de mecanismos de autenticação forte do cliente é o foco primordial da presente edição da *newsletter SEPA.pt*.

A obrigação de os prestadores de serviços de pagamento aplicarem autenticação forte a partir de 14 de setembro de 2019 implica que, ao longo dos próximos meses, alguns dos mecanismos de autenticação dos clientes (particulares e empresas) sejam adaptados, tornando-os compatíveis com os novos requisitos estabelecidos pela DSP2.

Assim, se em determinadas situações nos é, hoje em dia, apenas solicitado um código de utilizador e uma *password* para aceder ao *homebanking* ou para realizar uma determinada operação, a partir daquela data o nosso prestador de serviços de pagamento poderá passar a solicitar adicionalmente, por exemplo, a introdução de um código de autenticação que enviou naquele momento para o nosso telemóvel.

Neste enquadramento, para que a adoção dos novos mecanismos de autenticação forte ocorra com normalidade e simplicidade, é essencial que os prestadores de serviços de pagamento definam, o quanto antes, os procedimentos de autenticação forte que vão adotar a partir de setembro de 2019 e, adicionalmente, informem atempadamente os seus clientes das alterações que irão ser introduzidas.

Hélder Rosalino
Administrador do Banco de Portugal

Autenticação forte dos clientes

No dia 13 de março de 2018, foi publicado no *Jornal Oficial da União Europeia* o Regulamento Delegado (UE) 2018/389 da Comissão, de 27 de novembro de 2017, que suplementa a Diretiva (UE) 2015/2366, de 25 de novembro, relativa aos serviços de pagamento no mercado interno (DSP2[1]).

O Regulamento entra em vigor 18 meses após a sua publicação e estabelece normas técnicas de regulamentação relativas à autenticação forte do cliente e normas abertas de comunicação comuns e seguras que os prestadores de serviços de pagamento (PSP) têm de respeitar a partir dessa data.

1. A transposição da DSP2 para o ordenamento jurídico português foi efetuada com a publicação do Decreto-Lei n.º 91/2018, de 12 de novembro, que estabelece o novo Regime Jurídico dos Serviços de Pagamento e de Moeda Eletrónica.

Desse modo, a partir de 14 de setembro de 2019, os PSP terão de assegurar que os serviços de pagamento oferecidos por via eletrónica são prestados de forma segura, adotando tecnologias suscetíveis de garantir a autenticação segura do utilizador e de reduzir, tanto quanto possível, o risco de fraude. Para tal, os PSP deverão efetuar a autenticação forte dos seus clientes, sempre que estes i) acedam *online* à sua conta de pagamento; ii) iniciem uma operação de pagamento eletrónico, ou iii) realizem uma ação, através de um canal remoto, que possa envolver um risco de fraude no pagamento ou outros abusos.

A autenticação forte do cliente implica que os PSP, em todas as situações acima descritas, solicitem ao utilizador dois ou mais elementos pertencentes às categorias de "conhecimento" (por exemplo, uma palavra-passe), de "posse" (por exemplo, um código enviado por SMS para o telemóvel, provando, desta forma, a posse do dispositivo) e de "inerência" (uma característica que identifique o utilizador como a impressão digital), gerando, nesse momento, um código de autenticação único.

A partir de 14 de setembro, os PSP têm de fazer a autenticação forte dos clientes sempre que estes queiram aceder *online* à sua conta, iniciar um pagamento eletrónico ou realizar remotamente uma ação que possa envolver risco de fraude.

No entanto, a obrigação de os PSP aplicarem a autenticação forte do cliente não significa que a experiência do utilizador tenha de ser prejudicada. Na realidade, a autenticação forte já é muitas vezes utilizada quando interagimos com os PSP. Por exemplo, quando acedemos ao *homebanking* utilizando a chave móvel digital, quando recebemos um SMS com um código de autenticação para autorizar um pagamento, ou quando fazemos uma compra presencial numa loja com o cartão de pagamento, está já a ser aplicada autenticação forte.

Por outro lado, a adoção de novas tecnologias na prestação de serviços de pagamento, incluindo nos métodos de autenticação dos clientes, tem introduzido melhorias na comodidade, na facilidade e na rapidez com que as operações de pagamento são efetuadas.

Hoje em dia é possível comprovar a identidade de um cliente quando inicia um pagamento com a mesma facilidade com que se desbloqueia um *smartphone*, seja através de reconhecimento facial ou da leitura da impressão digital. Os elementos de autenticação da categoria "inerência", algo que é caraterístico e específico de cada pessoa, estão cada vez mais presentes no dia a dia dos utilizadores de serviços de pagamento. Num futuro não muito distante, será possível a utilização de outras soluções de autenticação, baseadas no reconhecimento da retina, da voz, do padrão de circulação sanguínea, ou mesmo dos batimentos cardíacos.

Embora a regra seja a obrigatoriedade de aplicar a autenticação forte do cliente, foram previstas situações – baseadas no nível de risco envolvido, no montante, na frequência e no canal através do qual a operação é executada – em que o PSP poderá optar por não solicitar autenticação forte do cliente. Nestas situações, o utilizador não pode ser responsabilizado caso a operação de pagamento venha a ser incorretamente executada, assumindo o PSP essa responsabilidade. São exemplos de isenções à aplicação da autenticação forte os pagamentos em portagens recorrendo a serviços como a Via Verde, as transferências a crédito efetuadas recorrentemente, para beneficiários frequentes, ou pagamentos abaixo de 30 euros que respeitem determinadas condições.

No comércio eletrónico, os PSP terão igualmente de aplicar as novas regras de autenticação forte do cliente no momento do pagamento. Assim, quando o cliente pretender concluir uma compra *online* e efetuar o pagamento ao comerciante, a operação de pagamento terá de ser autorizada com recurso a mecanismos de autenticação forte.

Com o objetivo de, simultaneamente, garantir a adoção de mecanismos de autenticação forte e proporcionar uma experiência mais simples e cómoda para o cliente na realização de compras *online*, os PSP têm procurado atualizar os seus procedimentos de autenticação, sobretudo na utilização de cartões de pagamento.

Neste sentido, as marcas internacionais de cartões, incluindo, entre outras, a *Mastercard* e a *Visa*, desenvolveram um protocolo (habitualmente designado EMVCo 3DS ou 3DS 2.0) para facilitar a conformidade com as novas regras da autenticação forte e melhorar a experiência do cliente.

A atual versão do protocolo (3DS 1.0), utilizada em alguns *sites* de comerciantes, é suportada pelo envio de um SMS para o telemóvel associado ao cartão de pagamento, com um código de autenticação único. Com a nova versão do protocolo, o banco emissor do cartão terá ao seu dispor um conjunto mais alargado de formas de autenticação que poderá utilizar, designadamente a leitura da impressão digital ou o reconhecimento facial.

Eventos recentes

- Comunicado do Banco de Portugal sobre a evolução das Transferências Imediatas em 2018, a 24 de janeiro.
- Publicação do *Estudo sobre os Custos Sociais dos Instrumentos de Pagamento em Portugal* (dados de 2017), a 28 de janeiro.
- Reunião plenária da Comissão Interbancária para os Sistemas de Pagamentos (CISP), na qual o incentivo à adoção de transferências imediatas foi um dos temas destacados, a 15 de março.
- Publicação do *Relatório dos Sistemas de Pagamentos* referente a 2018, a 29 de abril.

Eventos futuros

- Reunião interbancária sobre desenvolvimentos no mercado de pagamentos, a 17 de maio.
- Terceira *FinTech Meeting* do Banco de Portugal, a 23 de maio.
- Reunião plenária do Fórum para os Sistemas de Pagamentos, a 7 de junho.
- Reunião do Euro Retail Payments Board (ERPB), a 13 de junho.
- Reunião plenária da Comissão Interbancária para os Sistemas de Pagamentos (CISP), a 28 de junho.

Newsletter SEPA.pt • Banco de Portugal Av. Almirante Reis, 71 | 1150-012 Lisboa • www.bportugal.pt • Edição Departamento de Sistemas de Pagamentos | Área de Desenvolvimento e Regulação de Sistemas de Pagamentos • Design Departamento de Comunicação e Museu | Unidade de Design • ISSN 2182-2816 (*online*)