Guia sobre a autenticação forte do cliente

Pagamentos ainda mais seguros, a simplicidade de sempre

BANCO DE PORTUGAL
EUROSISTEMA

PAGAMENTOS MAIS SEGUROS A SIMPLICIDADE DE SEMPRE

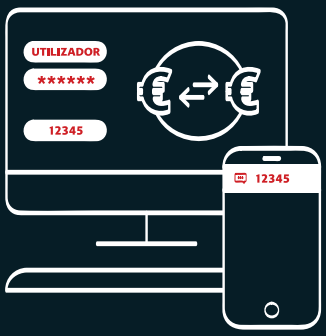
AUTENTICAÇÃO SIMPLES

\+

ELEMENTO ADICIONAL

=

AUTENTICAÇÃO FORTE



Enquadramento

Os serviços de pagamento eletrónicos têm novas regras, a pensar na sua segurança.

No dia 14 de setembro de 2019, entram em vigor em Portugal e nos outros Estados-Membros da União Europeia novas regras nos serviços de pagamento eletrónicos.

A partir dessa data, os prestadores de serviços de pagamento são obrigados a fazer a autenticação forte dos seus clientes sempre que estes acedam online à sua conta de pagamento, iniciem uma operação de pagamento eletrónico ou realizem uma ação, através de um canal remoto, que possa envolver risco de fraude no pagamento ou outros abusos.
As novas regras decorrem da entrada em vigor do 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, que tem aplicação direta nos Estados-Membros da União Europeia, 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), maioritariamente bancos, têm de respeitar a partir de 14 de setembro de 2019.

1 A DSP2 foi transposta para o ordenamento jurídico português 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.

Índice

A autenticação forte

1. O que é a autenticação do cliente?

A autenticação do cliente é o procedimento que permite ao prestador de serviços de pagamento/banco verificar a identidade de um utilizador ou a validade de utilização de um instrumento de pagamento específico.

2. O que torna a autenticação "forte"?

A autenticação do cliente é forte quando o procedimento de autenticação é efetuado com recurso a dois ou mais elementos pertencentes a, pelo menos, duas das seguintes categorias:

- Conhecimento (algo que só o utilizador conhece, por exemplo uma palavra-passe);
- Posse (algo que só o utilizador possui, por exemplo o seu telemóvel);
- Inerência (algo inerente ao utilizador e que o identifica, por exemplo uma impressão digital).

Estes elementos têm de ser independentes: o eventual comprometimento de um deles não pode pôr em causa a fiabilidade dos outros.

Por se considerar que as operações de pagamento remotas implicam um maior risco de fraude do que as operações presenciais, os PSP/bancos têm de garantir que, neste tipo de operações, a autenticação forte do cliente inclui um elemento adicional que associe de forma dinâmica a operação em causa ao montante e beneficiário específico.

Este requisito é muitas vezes cumprido através do envio de uma mensagem para o telemóvel do utilizador com um código criado especificamente para determinada operação de pagamento.

3. A partir de quando é exigida a autenticação forte do cliente?

Os requisitos de autenticação forte do cliente entraram em vigor a 14 de setembro de 2019. Nas compras com cartões de pagamento efetuadas através da internet estas regras não foram imediatamente aplicadas, pois foi definido um período de flexibilidade de supervisão.
As autoridades concederam aos prestadores de serviços de pagamento um período adicional – até 31 de dezembro de 2020 – para a adoção de mecanismos compatíveis com a autenticação forte, para minimizar o impacto destas alterações para os utilizadores.
A partir de 31 de dezembro de 2020, os prestadores de serviços de pagamento têm de aplicar autenticação forte às compras *online* com cartão. Veja também a resposta à questão 16. Posso continuar a usar os dados do meu cartão para fazer pagamentos *online*?

4. Em que situações é exigida a autenticação forte do cliente?

O PSP/banco terá de solicitar autenticação forte do cliente sempre que este último:

- Aceda a uma conta de pagamento através da internet (por exemplo, através do *homebanking* ou da aplicação móvel fornecida pelo PSP/banco, nomeadamente para consultar saldos ou movimentos da conta);
- Efetue uma operação de pagamento eletrónico (por exemplo, uma compra presencial com cartão de pagamento, uma transferência a crédito ordenada no *homebanking* ou uma compra *online*);
- Realize uma ação, através de um canal remoto, que possa envolver um risco de fraude no pagamento ou outros abusos (por exemplo, ao criar uma transferência recorrente a ser efetuada no início de cada mês ou alterar dados da conta).

5. O PSP/banco pode optar por não aplicar a autenticação forte do cliente?

Sim, em alguns casos. Embora a regra seja a obrigatoriedade de o PSP/banco 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/banco poderá optar por aceitar o acesso ou efetuar a operação sem solicitar autenticação forte ao cliente (aplicando uma isenção). São os casos das compras efetuadas com a tecnologia *contactless* e dos pagamentos efetuados em portagens com a Via Verde.

6. Em que situações o PSP/banco pode optar por não aplicar a autenticação forte do cliente?

O PSP/banco pode optar por não solicitar autenticação forte do cliente quando este último:

a. Acede a informação sobre contas de pagamento;

b. Inicia operações de pagamento sem contacto (*contactless*) no ponto de venda;

c. Utiliza terminais automáticos para o pagamento de tarifas de transporte e de estacionamento;

d. Inicia operações para uma lista de beneficiários considerados fiáveis (lista de beneficiários criada previamente);

e. Inicia operações recorrentes (lista de operações criada previamente);

f. Efetua transferências a crédito entre contas de um PSP/banco detidas pelo mesmo titular;

g. Inicia operações de pagamento de baixo valor;

h. Utiliza processos e protocolos de pagamento seguros (limitado a clientes empresa);

i. Inicia operações de pagamento que o PSP/banco considere terem reduzido risco.

7. Estarei menos protegido se o PSP/banco não me solicitar a autenticação forte?

Não, não estará menos protegido. O PSP/banco pode optar por não solicitar a autenticação forte do cliente caso considere que determinada operação não oferece risco significativo e se enquadra numa das isenções previstas.

Caso opte por não solicitar a autenticação forte do cliente, o PSP/banco assume quaisquer perdas financeiras decorrentes dessa operação, exceto se o cliente tiver atuado fraudulentamente.

Elementos que podem ser solicitados ao cliente

8. Que elementos da categoria de "conhecimento" me podem ser solicitados?

Podem ser considerados na categoria de conhecimento os elementos que respeitem a algo que só o utilizador conhece.

Elementos frequentemente partilhados com terceiros, como sejam os detalhes do cartão de pagamento, o contacto de *e-mail*, o *username* e o número de contrato associado ao acesso no *homebanking*, não são considerados "algo que só o utilizador conhece".

Lista de elementos de autenticação (não exaustiva)	Pode ser considerado elemento de conhecimento para a autenticação forte?
Palavra-passe	Sim
PIN	Sim
Padrão/caminho para desbloqueio do telemóvel	Sim
Username/número de contrato/ contacto de *e-mail*	Não
Detalhes de cartão de pagamento (impressos no cartão)	Não

Os PSP/bancos devem adotar medidas para reduzir o risco de os elementos da autenticação forte do cliente pertencentes à categoria de conhecimento serem descobertos por partes não autorizadas ou divulgados junto delas.

9. Que elementos da categoria de "posse" me podem ser solicitados?

Podem ser considerados na categoria de posse os elementos que respeitem a algo que só o utilizador possui.

Não podem ser classificados nesta categoria elementos que possam ser copiados ou reproduzidos, e cuja posse pelo cliente não possa ser comprovada no momento da autenticação. Desta forma, o cartão matriz, por ser facilmente replicável, não é considerado um elemento da categoria de posse.

Lista de elementos de autenticação (não exaustiva)	Pode ser considerado elemento de posse para a autenticação forte?
Dispositivo do cliente cuja posse é comprovada pela geração/receção de uma palavra-passe de utilização única (*hardware/software token*; receção de uma mensagem no telemóvel)	Sim
Dispositivo do cliente que gera uma assinatura digital (*hardware/software token*)	Sim
Cartão introduzido num leitor físico	Sim
Detalhes de cartão de pagamento (impressos no cartão)	Não
Cartão matriz	Não

Os PSP/bancos devem adotar medidas para reduzir o risco de os elementos da autenticação forte do cliente pertencentes à categoria de posse serem utilizados por partes não autorizadas.

10. Que elementos da categoria de "inerência" me podem ser solicitados?

Podem ser considerados na categoria de inerência os elementos que respeitem a algo que só o utilizador é.

Lista de elementos de autenticação (não exaustiva)	Pode ser considerado elemento de inerência para a autenticação forte?
Reconhecimento de impressão digital	Sim
Reconhecimento de voz	Sim
Reconhecimento facial	Sim
Reconhecimento de retina	Sim
Reconhecimento de batimento cardíaco	Sim
Padrão/caminho para desbloqueio do telemóvel	Não

Os PSP/bancos devem adotar medidas para reduzir o risco de os elementos de autenticação pertencentes à categoria de inerência e lidos pelos dispositivos e *software* de acesso fornecidos ao ordenante serem descobertos por partes não autorizadas. No mínimo, os prestadores de serviços de pagamento devem assegurar que tais dispositivos e *software* de acesso implicam uma probabilidade muito reduzida de uma parte não autorizada ser autenticada como sendo o ordenante.

11. Que procedimentos de autenticação podem continuar a ser utilizados? E quais serão descontinuados?

Para que se considere que foi aplicada autenticação forte do cliente é necessário que a autenticação seja efetuada com recurso a dois ou mais elementos pertencentes a, pelo menos, duas categorias distintas.

Alguns dos procedimentos de autenticação até agora aplicados já eram compatíveis com os requisitos regulamentares e podem continuar a ser utilizados.

Por exemplo, a utilização de uma palavra-passe (elemento de conhecimento) conjuntamente com uma mensagem enviada para o telemóvel com um código (elemento de posse) poderá continuar a ser utilizado para efeitos de autenticação forte.

Contudo, alguns procedimentos de autenticação não poderão ser utilizados pelos PSP/bancos para efeitos de autenticação forte do cliente.

Por exemplo, as situações em que é utilizada uma palavra-passe (elemento de conhecimento) e um conjunto de coordenadas do cartão-matriz (não é considerado elemento de autenticação forte) não cumprem os novos requisitos estabelecidos. O cartão matriz, por ser replicável, deixa de ser um elemento válido para efeitos de aplicação de autenticação forte do cliente.

Também os detalhes impressos no cartão de pagamento (designadamente o número do cartão, a data de validade e o código CVV/CVC) não poderão ser utilizados para fins de autenticação forte do cliente. Neste caso, por serem frequentemente partilhados com terceiros.

No entanto, a informação do cartão matriz e os detalhes impressos no cartão de pagamento podem continuar a ser utilizados como complemento à autenticação forte ou em operações que não requeiram a autenticação forte do cliente.

Lista de procedimentos de autenticação (não exaustiva)

Conhecimento	Posse
PIN	Cartão de pagamento com *chip* num terminal **(em loja)**
Palavra-passe	Código enviado por mensagem
	Aplicação instalada no telemóvel do cliente
Palavra-passe	Código gerado por *hardware/ software token*
Palavra-passe	
PIN + Palavra-passe	
Palavra-passe	
Assinatura digital gerada por *hardware/ software token*	
	Código enviado por mensagem
Detalhes de cartão de pagamento virtual MBnet **(número do cartão + data de validade + CVV/CVC)**	Código enviado por mensagem

Inerência	Outros elementos	Pode ser considerado como procedimento de autenticação forte?
		Sim
		Sim
Reconhecimento de impressão digital		Sim
		Sim
	Username	Não O *username* não é considerado elemento válido para efeitos de autenticação forte.
		Não Estes elementos são da mesma categoria.
	Coordenadas de cartão-matriz	Não O cartão matriz não é considerado elemento válido para efeitos de autenticação forte.
Reconhecimento facial		Sim
	Detalhes de cartão de pagamento **(número do cartão + data de validade + CVV/CVC)**	Não Os detalhes impressos no cartão não são considerados elementos válidos para efeitos de autenticação forte.
		Sim Mas apenas para a primeira compra.

Homebanking

12. A autenticação forte ser-me-á exigida sempre que quiser aceder ao *homebanking*?

Não. Os PSP/bancos são sempre obrigados a aplicar autenticação forte do cliente na primeira vez em que este acede ao *homebanking*. Nos 90 dias seguintes, poderão optar por fazer uma autenticação mais simples. Decorrido este período de 90 dias, o PSP/banco terá de solicitar novamente a autenticação forte do cliente quando este aceder à conta de pagamento.

13. Para aceder ao *homebanking*, foi aplicada a autenticação forte. Para realizar um pagamento, vão solicitá-la novamente?

Sim, uma vez que ambas as ações (acesso à conta de pagamento através da internet e realização de uma operação de pagamento eletrónico) obrigam à aplicação de autenticação forte do cliente pelo PSP/banco.

No entanto, será possível ao PSP/banco reutilizar elementos de autenticação forte na mesma sessão.

Assim, se, por exemplo, no acesso ao *homebanking* for solicitado uma palavra-passe (elemento de conhecimento) e um código enviado por mensagem para o telemóvel (elemento de posse), o PSP/banco poderá reutilizar um destes elementos caso o cliente pretenda efetuar um pagamento durante essa mesma sessão.

Neste caso, o PSP/banco poderá, por exemplo, reutilizar a palavra-passe (elemento de conhecimento) introduzida pelo cliente aquando do acesso ao *homebanking* e solicitar apenas a introdução de um novo código enviado por mensagem (elemento de posse) para o utilizador, aquando da realização da operação de pagamento.

Este processo evita que, na mesma sessão, o cliente tenha de introduzir duas vezes o mesmo elemento de autenticação.

14. Costumo autenticar-me utilizando informação do cartão matriz. Poderei continuar a fazê-lo como até aqui?

Não. A partir de 14 de setembro, o PSP/banco não poderá utilizar o cartão matriz na autenticação forte do cliente. O cartão matriz poderá, no entanto, continuar a ser utilizado como complemento da autenticação forte ou para autenticar os utilizadores em operações que não requeiram autenticação forte.

Pagamentos *online*

15. O que muda nos pagamentos *online*?

A partir de 14 de setembro, os PSP/bancos terão de solicitar a autenticação forte dos clientes nas operações de pagamento *online*. Ver resposta à questão 2. O que torna a autenticação "forte"?

Por se considerar que as operações de pagamento remotas implicam um maior risco de fraude do que as operações presenciais, os PSP/bancos têm de garantir que, neste tipo de operações, a autenticação forte do cliente inclui um elemento adicional que associe de forma dinâmica a operação em causa ao montante e beneficiário específico.

Este requisito é muitas vezes cumprido através do envio de uma mensagem para o telemóvel do utilizador com um código criado especificamente para determinada operação de pagamento.

16. Posso continuar a utilizar os dados do meu cartão para fazer pagamentos *online*?

Até 31 de dezembro de 2020 os PSP/bancos usufruíram de um período de flexibilidade supervisiva na aplicação das regras de autenticação forte do cliente nas compras *online* com cartão. Por isso, entre 14 de setembro de 2019 e esta data, foi permitido ao cliente continuar a utilizar unicamente os dados do cartão para fazer pagamentos *online*.

Contudo, os detalhes impressos nos cartões de pagamento, como seja o número do cartão, a data de validade ou o código CVV/CVC não são considerados elementos válidos de autenticação forte do cliente, pelo que não serão suficientes para realizar pagamentos *online* a partir de 31 de dezembro de 2020.

Os PSP/bancos desenvolveram procedimentos alternativos de autenticação forte do cliente especificamente para compras na internet. Estes novos procedimentos de autenticação podem incluir, por exemplo, a leitura de impressões digitais ou reconhecimento facial, a utilização de palavras-passe ou PIN associados ao cartão, ou a receção de uma mensagem com um código que comprove a posse de um telemóvel associado ao cliente.

A partir de 31 de dezembro de 2020, a aplicação de autenticação forte do cliente nos pagamentos *online* com cartão é obrigatória. Informe-se junto do(s) seu(s) PSP/banco(s) para perceber quais as soluções disponibilizadas para a autenticação forte do cliente e quais os procedimentos que deve seguir, como seja a instalação de aplicações móveis ou a familiarização com outros mecanismos de autenticação.

Pagamentos presenciais

17. O que muda nos pagamentos presenciais?

A autenticação forte do cliente também se aplica a pagamentos presenciais, desde que sejam eletrónicos.

No entanto, muitos dos procedimentos de autenticação utilizados atualmente em pagamentos presenciais eletrónicos, por exemplo nas compras com cartão, já preenchem os requisitos de autenticação forte do cliente, pelo que é possível que os clientes não sintam diferenças ao realizarem a maioria das operações. O cartão físico, cuja posse é confirmada pelo *chip* EMV presente no cartão, conjuntamente com o PIN que só o cliente conhece, respeita os requisitos exigidos pelo novo enquadramento regulamentar.

É de realçar, no entanto, que os pagamentos com recurso à banda magnética do cartão, sem a utilização de *chip* EMV, não satisfazem os requisitos de autenticação forte do cliente.

18. Posso continuar a fazer pagamentos *contactless* sem introduzir o PIN?

Sim. Os pagamentos com recurso à tecnologia *contactless* mantêm as atuais facilidades de utilização. De forma a equilibrar a facilidade de uso para os clientes com a segurança nas operações, continuará a ser possível fazer pagamentos *contactless* sem introduzir o PIN em operações até 50 euros, desde que não tenham sido efetuadas mais de 5 operações ou que o valor total das operações sem autenticação forte não ultrapasse os 150 euros acumulados.

Os PSP/bancos podem definir limites inferiores para a realização de pagamentos *contactless* sem introduzir o PIN.

Outras operações

19. Posso continuar a pagar portagens com recurso à Via Verde, como habitualmente?

Sim. Os pagamentos efetuados em portagens ou parques de estacionamento recorrendo à Via Verde, ou soluções similares, continuarão a ser feitos como até aqui. Estes pagamentos

enquadram-se na isenção "terminais automáticos para o pagamento de tarifas de transporte e de estacionamento. Para mais informações sobre as isenções, consulte a resposta à questão 6. Em que situações o prestador de serviços de pagamento pode optar por não aplicar a autenticação forte do cliente?

20. Posso continuar a fazer débitos diretos como habitualmente?

Sim. Os pagamentos eletrónicos iniciados exclusivamente pelo beneficiário, como é o caso dos débitos diretos e de determinadas operações de pagamento com cartão, não requerem a autenticação forte do cliente.

Contacte o seu banco e atualize os seus dados