Comunicação Comum e Segura e Autenticação Forte – Ponto de Situação –

Departamento de Sistemas de Pagamentos

Reunião Interbancária | 18 novembro 2019

BANCO DE PORTUGAL
EUROSISTEMA

AGENDA

- Enquadramento
- Autenticação forte do cliente
- Autenticação forte do cliente no âmbito do comércio eletrónico
- Normas abertas de comunicação comuns e seguras

AGENDA

- Enquadramento
- Autenticação forte do cliente
- Autenticação forte do cliente no âmbito do comércio eletrónico
- Normas abertas de comunicação comuns e seguras

Enquadramento

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

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**). Esta Diretiva 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.

AGENDA

- Enquadramento
- **Autenticação forte do cliente**
- Autenticação forte do cliente no âmbito do comércio eletrónico
- Normas abertas de comunicação comuns e seguras

Autenticação forte do cliente

A partir de 14 de setembro de 2019

O que é a autenticação forte?

A autenticação do cliente implica que o PSP/banco solicite ao utilizador **dois ou mais elementos pertencentes às categorias** de:

Conhecimento

Posse

Inerência

Em que situações é exigida?

Acesso *online* a conta de pagamento

Pagamento eletrónico

Ação remota que possa envolver risco de fraude ou abuso

Para **operações de pagamento remotas** (efetuadas, por exemplo, através da internet), a autenticação forte tem de incluir também elementos que associem de **forma dinâmica** a operação a um montante e beneficiário específico.

AGENDA

- Enquadramento
- Autenticação forte do cliente
- **Autenticação forte do cliente no âmbito do comércio eletrónico**
- Normas abertas de comunicação comuns e seguras

Autenticação forte do cliente no âmbito do comércio eletrónico

1 ***EBA Opinion on the elements of strong customer authentication*** **(jun-19)**

Tendo em conta as dificuldades de migração encontradas pelo mercado Europeu para aplicar SCA nas compras *online* baseadas em cartão de pagamento, foi considerada a possibilidade de as NCA mostrarem flexibilidade quanto à aplicação de SCA neste âmbito.

2 **Questionários da EBA disseminados pelas NCA**

A EBA preparou questionários direcionados aos intervenientes de mercado com vista a avaliar o nível de preparação do mercado e tomar uma decisão sustentada quanto ao prazo final para a aplicação de SCA no comércio eletrónico.

3 ***EBA Opinion on the deadline and process for completing the migration to SCA for e-commerce card-based payment transactions*** **(out-19)**

A EBA definiu a data de **31 de dezembro de 2020** como prazo final para a plena migração para soluções de SCA no âmbito do comércio eletrónico e estabeleceu que as NCA devem acompanhar a implementação dos planos de migração dos PSP.

Autenticação forte do cliente no âmbito do comércio eletrónico

O Banco de Portugal comunicou, em 17 de outubro de 2019, que iria adotar a flexibilidade prevista no parecer da EBA e monitorizar o cumprimento dos planos de migração dos PSP

Enquadramento

Tabelas 1 e 2 da *Opinion* da EBA:

- Conjunto de etapas e prazos definidos pela EBA para a monitorização pelas NCA.

Metodologia

Através de 8 questionários:

- 4 dirigidos aos PSP emitentes de cartões
- 4 dirigidos aos PSP adquirentes de operações

Atualizações regulares dos questionários.

Plano de ação

Envio de questionários para resposta.

Reporte trimestral pela NCA à EBA.

Endereço eletrónico para confirmação/comunicação dos interlocutores até 22 de novembro de 2019: sp.psd2@bportugal.pt

Autenticação forte do cliente no âmbito do comércio eletrónico

Questionários | PSP emitentes de cartões

Questionário 1

- Informação quanto ao **plano de comunicação com os PSU** relativamente aos procedimentos de SCA, isenções e transações fora de âmbito de SCA

Questionário 2

- Identificação dos **procedimentos de autenticação** disponibilizados
- Descrição dos **planos de migração** para soluções compatíveis com SCA

Questionário 3

- Descrição do **nível de preparação** para aplicação de SCA, mediante apresentação de indicadores

Questionário 4

- Confirmação da **finalização da execução dos planos de migração**

Autenticação forte do cliente no âmbito do comércio eletrónico

Questionários | PSP adquirentes de operações

Questionário 5

- Informação quanto ao **plano de comunicação com os comerciantes** relativamente às alterações necessárias às tecnologias utilizadas para que sejam compatíveis com os requisitos de SCA

Questionário 6

- Identificação das **tecnologias** disponibilizadas
- Descrição dos **planos de migração** para tecnologias compatíveis com SCA

Questionário 7

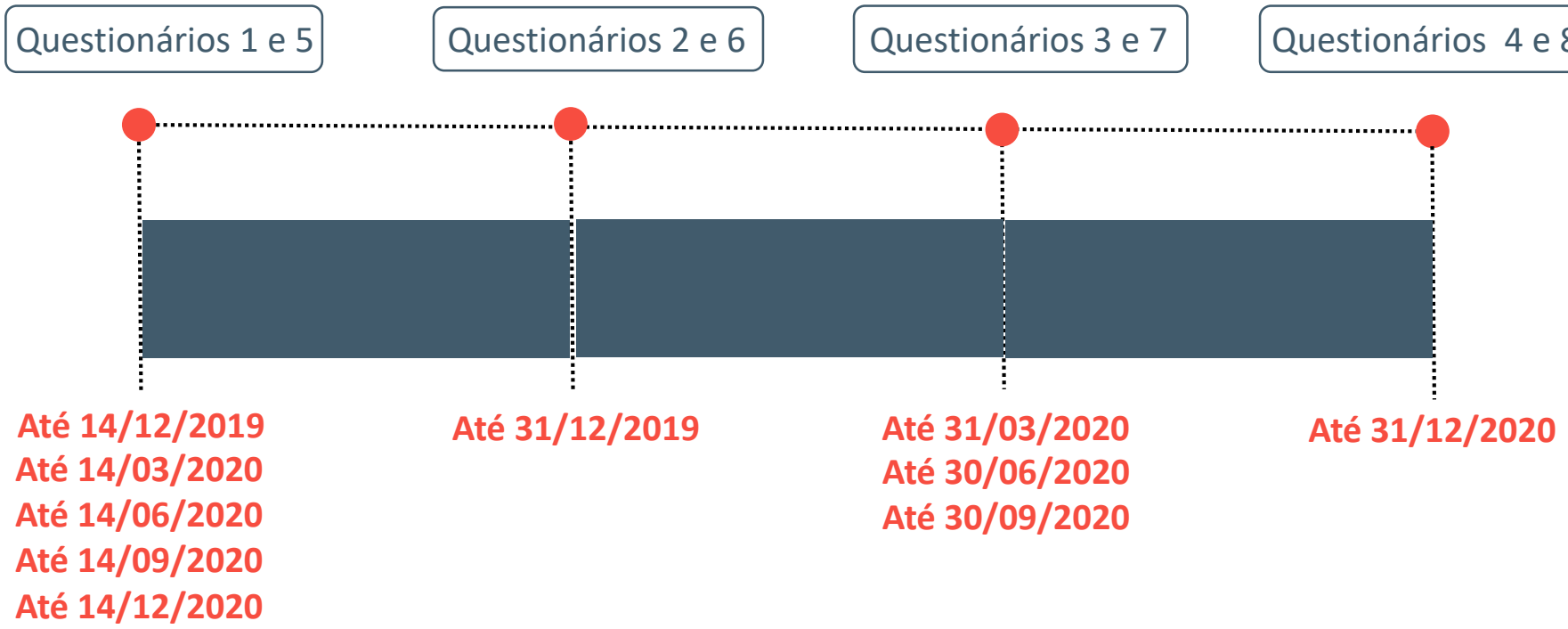
- Descrição do **nível de preparação** para aplicação de SCA, mediante apresentação de indicadores

Questionário 8

- Confirmação da **finalização da execução dos planos de migração**

Autenticação forte do cliente no âmbito do comércio eletrónico

Quais os prazos para remeter os questionários ao Banco de Portugal?



AGENDA

- Enquadramento
- Autenticação forte do cliente
- Autenticação forte do cliente no âmbito do comércio eletrónico
- **Normas abertas de comunicação comuns e seguras**

Normas de comunicação comuns e seguras

A partir de 14 de setembro de 2019

Novos serviços de pagamento

Com a DSP2, passaram a estar consagrados e regulados dois novos serviços de pagamento:

1. **Serviços de informação sobre contas**
2. **Serviços de iniciação de pagamentos**

Implicações

Os PSP têm de:

- Disponibilizar uma **interface dedicada** (API) ou
- **Adaptar o seu *homebanking***

Monitorização contínua do BdP

- Realização de questionários
- Acompanhamento de reclamações e pedidos de informação
- Análise de eventuais denúncias
- Realização de testes diretos às API do ponto de vista do utilizador
- Verificação *in loco* dos requisitos
- Emissão de recomendações

Normas de comunicação comuns e seguras

Monitorização | Instrumentos de pagamento

Os TPP devem poder iniciar operações recorrendo a **todos os instrumentos de pagamento** disponibilizados pelos ASPSP nos canais dos seus clientes.

Os ASPSP não estão a disponibilizar alguns instrumentos de pagamento. Por exemplo: “Pagamentos de serviços”, “Pagamentos ao Estado”, “Pagamentos à Segurança Social”, “Carregamentos”, “Pagamentos em Lote”, “Envio de ficheiros de Pagamentos”.

Todos os instrumentos de pagamento oferecidos nos canais para acesso direto dos clientes devem também estar disponíveis na interface dedicada, o mais tardar até ao final do primeiro trimestre de 2020.

Normas de comunicação comuns e seguras

Monitorização | Fluxo de autenticação

O desenho da interface dedicada **não deverá conduzir a atritos desnecessários** na experiência disponibilizada aos PSU quando acedem à sua conta ou a quaisquer outros atributos através de um TPP, suscetível de dissuadir direta, ou indiretamente, os PSU de utilizar os serviços do TPP.

Foram identificadas mensagens que solicitam confirmação de consentimentos, que são relativas a riscos de fraude ou outras mensagens/passos não associados ao processo de autenticação.

Solicitámos que cada instituição enviasse ao BdP *print screens* do seu processo sequencial de autenticação.

BdP detetou situações de: i) pedidos de confirmação de consentimento, ii) referência a perguntas e respostas frequentes e iii) outras validações desnecessárias.

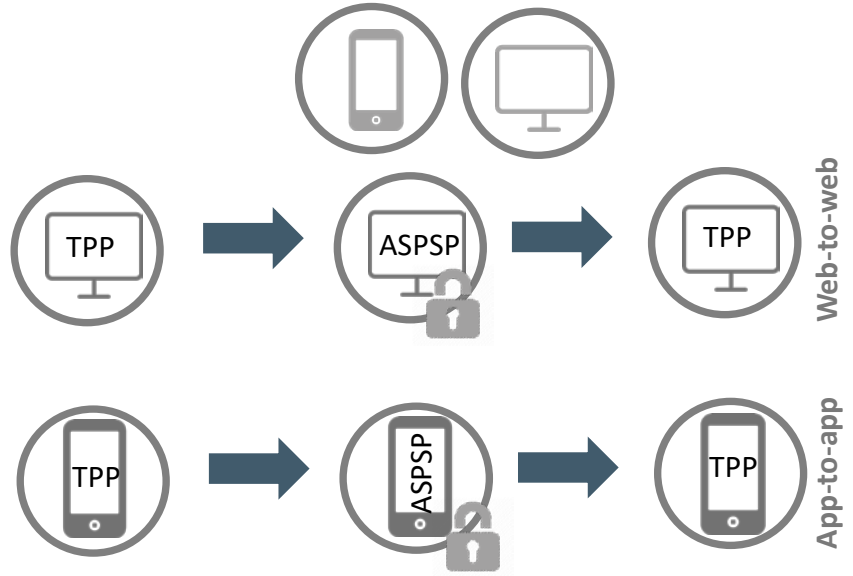
Cada instituição deverá confirmar que o seu processo de autenticação cumpre com os requisitos e que eventuais mensagens desencorajadoras/validações desnecessárias foram retiradas.

Normas de comunicação comuns e seguras

Monitorização | Canais de autenticação

As interfaces disponibilizadas devem **permitir que os TPP recorram a todos os procedimentos de autenticação facultados pelo ASPSP ao PSU.**

Não estará a ser disponibilizada *app-to-app redirect.*



ASPSP que usam o método *redirect* e possibilitam a autenticação via a app do telemóvel diretamente aos seus clientes, devem suportar *app-to-app redirect* quando o cliente recorre a um TPP.

Comunicação Comum e Segura e Autenticação Forte – Ponto de Situação –

Departamento de Sistemas de Pagamentos

Reunião Interbancária | 18 novembro 2019

BANCO DE PORTUGAL
EUROSISTEMA