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

Departamento de Sistemas de Pagamentos

Reunião Interbancária | 18 junho 2020

BANCO DE PORTUGAL
EUROSISTEMA

AGENDA

- Autenticação forte do cliente
- Normas abertas de comunicação comuns e seguras

AGENDA

- Autenticação forte do cliente
- Normas abertas de comunicação comuns e seguras

Autenticação forte do cliente – 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 ***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.

Interno - Banco de Portugal

Autenticação forte do cliente – comércio eletrónico

O Banco de Portugal comunicou, em 17 de outubro de 2019, que iria adotar a flexibilidade prevista na *Opinion* 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 pelas NCA à EBA e numa base *ad-hoc*, sempre que a EBA o solicitar.

A data limite para a aplicação de SCA no comércio eletrónico com cartão é 31 de dezembro de 2020.

Interno - Banco de Portugal

Autenticação forte do cliente – comércio eletrónico

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

Legenda:
Já respondido
Enviado, aguarda resposta
Cancelado
Não enviado

Interno - Banco de Portugal

Autenticação forte do cliente – comércio eletrónico

Atualmente, encontram-se para resposta os questionários 3 e 7

Qual o nível de preparação dos PSP emissores e adquirentes para a aplicação de SCA no âmbito do comércio eletrónico?

Dados: 14/09/2019 a 13/06/2020

Os PSP devem responder até **30 de junho de 2020** (via epsilon)

TÓPICOS

1. Número de transações compatíveis com SCA;
2. Número de transações onde uma isenção foi aplicada;
3. Número de transações fora do âmbito de SCA;
4. Número de transações fraudulentas;
5. Implementação do protocolo 3DS;
6. …

Interno - Banco de Portugal

Autenticação forte do cliente – comércio eletrónico

Plano Nacional de Migração

- Da autoria do Fórum para os Sistemas de Pagamentos
- Calendariza um conjunto de iniciativas e ações
- Que devem ser adotadas pelos vários agentes de mercado em Portugal (PSP, comerciantes e associações setoriais e representativas dos consumidores)
- Com o objetivo de promover uma implementação consistente dos novos requisitos de autenticação forte no comércio *online* até à data-limite definida pela EBA

A publicar brevemente

Interno - Banco de Portugal

AGENDA

- Autenticação forte do cliente
- **Normas abertas de comunicação comuns e seguras**

Normas de comunicação comuns e seguras

Desde 14 de setembro de 2019

Os PSP têm de:

- Disponibilizar uma **interface dedicada** (API) ou
- **Adaptar os canais dos clientes** (*homebanking/app)*

para permitir a comunicação com os TPP

Monitorização contínua do BdP

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

Em caso de desconformidades com a regulamentação aplicável

- **Revogação da isenção** do mecanismo de contingência
- **Coimas** entre 10 000 euros e 5 000 000 euros

Interno - Banco de Portugal

Normas de comunicação comuns e seguras

Monitorização | 1. Instrumentos de pagamento

Os TPP devem poder iniciar operações recorrendo a <u>todos os instrumentos de pagamento</u> disponibilizados pelos ASPSP nos canais dos seus clientes

Os ASPSP não disponibilizaram à data de 14 de setembro de 2019, e em alguns casos continuam a não disponibilizar, alguns instrumentos de pagamento nas API. Por exemplo: "Pagamentos ao Estado", "Pagamentos à Segurança Social", "Carregamentos", "Pagamentos em Lote", "Envio de ficheiros de Pagamentos".

1. REVISÃO DO PLANO DE DISPONIBILIZAÇÃO DOS INSTRUMENTOS
2. COMUNICAÇÃO DO PLANO AO BANCO DE PORTUGAL

Interno - Banco de Portugal

Normas de comunicação comuns e seguras

Monitorização | 1. Instrumentos de pagamento

A disponibilização de um novo instrumento de pagamento nos canais diretamente acessíveis pelos clientes implica a sua disponibilização **simultânea** na API.

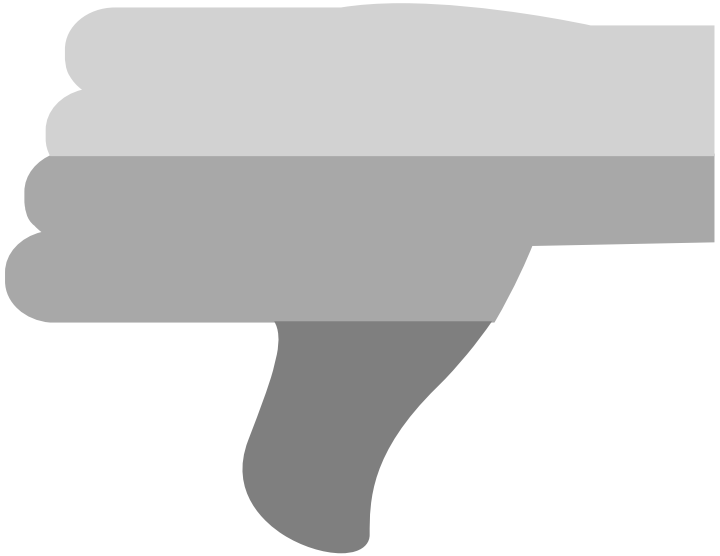
Os TPP devem disponibilizar na API **todos os instrumentos de pagamento** oferecidos diretamente aos clientes nos prazos indicados ao Banco de Portugal.

Interno - Banco de Portugal

Normas de comunicação comuns e seguras

Monitorização | 2. Fluxo de autenticação

O desenho da interface dedicada não deverá conduzir a **atritos desnecessários** na experiência dos PSU quando acedem à sua conta ou a quaisquer outros serviços através de um TPP, que sejam suscetíveis de dissuadir direta, ou indiretamente, os PSU de utilizar os serviços do TPP



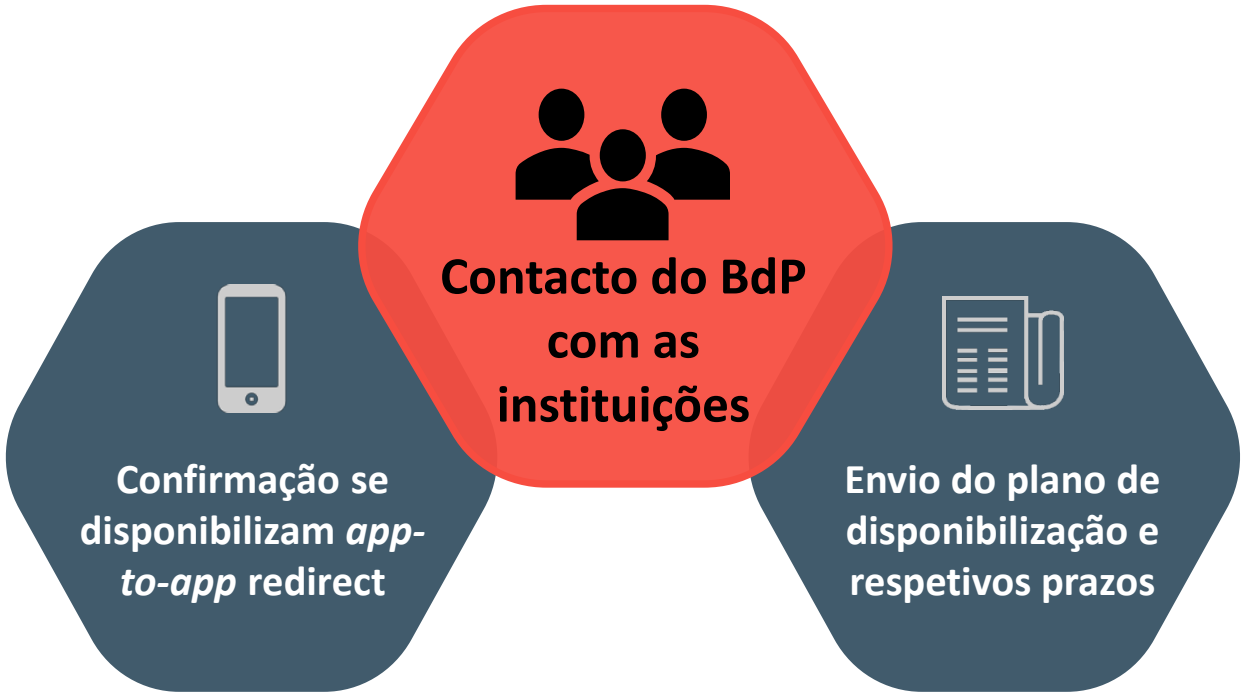
1. Duplicação da informação sobre conta ou da operação de pagamento
2. Linguagem alarmista particularmente alusiva ao consentimento
3. FAQ e outras mensagens não diretamente relacionadas com a autenticação
4. Confirmações adicionais do consentimento

Situações mais concretas de obstáculos têm sido discutidas a nível europeu. O Banco de Portugal tem acompanhado as discussões, pelo que irá, oportunamente, contactar os ASPSP.

Interno - Banco de Portugal

Normas de comunicação comuns e seguras

Monitorização | 3. Canais de autenticação



Berlin Group *Guidelines*

SIBS *Guidelines*

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.

Interno - Banco de Portugal

Normas de comunicação comuns e seguras

Monitorização | 3. Canais de autenticação

Novos procedimentos de autenticação acessíveis diretamente pelos clientes devem também ser disponibilizados na API.

Os ASPSP devem disponibilizar na API todos os processos de autenticação que oferecem diretamente aos seus clientes (p.ex. *browser to app;* procedimentos de autenticação no ponto de venda físico; entre outros).

Interno - Banco de Portugal

Normas de comunicação comuns e seguras

Monitorização | 4. Análise de reclamações – Erros API

TPP a operar no mercado português apontam **dificuldades no acesso às API**. A maioria dos problemas reportados referem-se a falhas no processo de autenticação.

Possíveis causas apontadas:

- PSU não introduzem a OTP
- PSU introduzem *username/n.º* de contrato errados
- **OTP não é entregue ao PSU**
- **Processo de autenticação complexo**
- **Interfaces dos ASPSP inacessíveis**
- **Redireccionamentos não funcionam de forma adequada**
- **Erros técnicos de sistema**

? **Desagregação entre:**
- **erros imputáveis ao PSU**
- **erros da API**

Cada instituição deverá **interagir com os TPP de uma forma construtiva** para resolver os problemas identificados sem demora. O **BdP vai solicitar aos ASPSP informação detalhada** sobre os erros que os TPP têm obtido no acesso à API.

Interno - Banco de Portugal

Normas de comunicação comuns e seguras

Monitorização | 5. Publicação de estatísticas

Cada ASPSP que tenha beneficiado da isenção do mecanismo de contingência deve possuir um plano para a **publicação trimestral de estatísticas diárias** sobre a disponibilidade e o desempenho da API e de cada uma das interfaces disponibilizadas diretamente aos seus próprios clientes.

Foram identificadas situações de estatísticas atrasadas, *links* inválidos ou estatísticas incompletas.

O BdP remeteu um e-mail aos ASPSP a solicitar a regularização da informação estatística

Os *links* deverão ser enviados ao Banco de Portugal, bem como as estatísticas publicadas, assegurando a publicação atempada das estatísticas.

Interno - Banco de Portugal

Normas de comunicação comuns e seguras

Monitorização | *EBA Opinion on the obstacles under Article 32(3) of the RTS on SCA and CSC*

A EBA publicou no passado dia 4 de junho uma *Opinion* sobre os obstáculos à prestação de serviços de iniciação de pagamentos e de serviços de informação sobre contas na API

Procedimentos de autenticação

A API deverá suportar os mesmos procedimentos de autenticação oferecidos nas interfaces diretamente acessíveis pelos PSU.

Redirecionamento no ponto de venda

A API deverá permitir a realização de pagamentos no ponto de venda físico, através de um PISP, caso o ASPSP permita que tal aconteça nas interfaces diretamente acessíveis pelos PSU.

Múltiplas SCA

A API não deverá solicitar mais SCA do que aquelas solicitadas diretamente ao PSU em situações comparáveis.

Interno - Banco de Portugal

Normas de comunicação comuns e seguras

Monitorização | *EBA Opinion on the obstacles under Article 32(3) of the RTS on SCA and CSC*

A EBA publicou no passado dia 4 de junho uma *Opinion* sobre os obstáculos à prestação de serviços de iniciação de pagamentos e de serviços de informação sobre contas na API

Reautenticação 90 dias

A API deverá permitir que o TPP beneficie da isenção de aplicação de SCA no acesso a informação sobre contas (artigo n.º 10 do RD).

Seleção de contas

A API não deverá obrigar à introdução manual do IBAN no ambiente do TPP.

Caso o TPP não transmita o IBAN na chamada à API, o ASPSP deverá permitir que o PSU selecione a conta no processo de SCA do ASPSP.

Confirmações adicionais

O pedido de confirmação do consentimento pelo PSU é um obstáculo.

Os ASPSP não deverão impor confirmações adicionais em contas corporativas.

O PSU pode solicitar ao ASPSP que seja solicitado SCA no próximo acesso.

Registos adicionais

É um obstáculo o ASPSP solicitar ao TPP registos adicionais que vão além do que é tecnicamente necessário.

No entanto, a troca de informação poderá ser tecnicamente necessária.

Interno - Banco de Portugal

Normas de comunicação comuns e seguras

Monitorização | *EBA Opinion on the obstacles under Article 32(3) of the RTS on SCA and CSC*

O Banco de Portugal irá promover a realização de um *workshop* onde se irão analisar em detalhe, entre outros temas, as clarificações trazidas pela *Opinion*.

A data da sua realização será brevemente comunicada.

Interno - Banco de Portugal

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

Departamento de Sistemas de Pagamentos

Reunião Interbancária | 18 junho 2020

BANCO DE PORTUGAL
EUROSISTEMA