

15º Fórum Pix

GT SEG

Pagamentos Instantâneos



**BANCO CENTRAL
DO BRASIL**

GT de Segurança I Motivadores, participantes e metodologia

Contexto

O GT SEG é um grupo de trabalho coordenado pelo Banco Central e secretariado pela FEBRABAN em que as associações abaixo participam colaborando com o debate.

Objetivos

Apresentar os aspectos de segurança mapeados que necessitam alguma revisão e novos riscos identificados, com seus respectivos planos de ação.

Ciclos de contribuições

Início das reuniões em dezembro de 2019



9º Ciclo – Apresentação no
15º Fórum PI – Setembro/21

Participantes*

1. ABBC
2. ABECS
3. ABIPAG
4. ABO2O
5. ABRACAM

6. ABRANET
7. AGEV
8. AMPEF
9. FEBRABAN
10. PAGOS

11. ZETTA
12. PSTI ABBC
13. PSTI C&M SOFTWARE
14. PSTI JD
15. SINDTELEBRASIL

16. TESOURO NACIONAL
17. B3
18. CIP
19. Claro
20. RTM

* Participantes aprovados pelo Banco Central

AGENDA do 9º Ciclo – Julho, Agosto e Setembro

- 1 > Consulta Pública QR Code do Pagador
- 2 > Notificação de infração – identificação do ITP

GT de Segurança | Consulta sobre o QR Code do Pagador

Consulta Pública enviada: 10/08/2021

Discussão GT Seg: 19/08/2021

Resposta do GT Seg: 23/08/2021

Considerações do GT SEG:

- De acordo com o modelo de negócio e especificação técnica proposta, vislumbramos dois momentos nos quais devem ser consideradas **potenciais vulnerabilidades de segurança: (i) geração do QR Code num contexto offline e (ii) pagamento com a leitura do QR Code gerado offline** pelo recebedor.
- Num contexto offline, contudo, as validações para garantir que um determinado QR Code foi efetivamente gerado em um determinado dispositivo ainda não são possíveis de forma segura pelas **tecnologias utilizadas atualmente pelos participantes**, pois seria necessário armazenar toda a lógica de autenticação no dispositivo, gerando um risco de segurança significativo para todas as demais funcionalidades e produtos contratados pelo cliente.
 - Em contrapartida, desenvolver funcionalidades e senha específica para a utilização do Qr Code offline requer **investimentos e prazo de desenvolvimento significativos**.
- Ainda existem lacunas não pacificadas, como por exemplo a impossibilidade de o PSP do pagador oferecer ao seu cliente **uma confirmação em tempo real** do que efetivamente foi pago. A **experiência para o usuário pagador fica significativamente degradada**, tornando-o refém da boa-fé do usuário recebedor.
- Adicionalmente, alguns cenários precisam **de um maior tempo** para aprofundar os estudos de possíveis riscos, como por exemplo, no QR Code Offline da configuração avançada, garantir que o pagamento será realizado de fato pelo titular ou autorizado por ele.
- Dessa forma, recomendamos inicialmente focar no QR Code **básico**, considerando o prazo de desenvolvimento suficiente para adequação de infraestrutura, assim como, manter em um segundo o QR Code Offline da **configuração avançada**, devido a necessidade de **maior tempo para aprofundar os estudos de possíveis riscos e segurança necessária para o seu funcionamento**.

As respostas na íntegra foram entregues ao Banco Central no dia 23/08/2021.

GT de Segurança | Pleito: Notificação de Infração – Identificar o ITP

Proposta: Identificar o ITP (Iniciador de Transação de Pagamento) no momento da notificação de infração

Contexto: Com a entrada da **Fase 3 do Open Banking** em 29 de Out., haverá transações PIX originadas pelo ITP (Iniciador de Transação de Pagamento). Para que seja possível identificar de forma clara a origem da transação e ter uma visão completa sobre possíveis fraudes, o grupo solicita a criação de um **novo domínio**.

Adicionar um **novo domínio** no campo motivo no Payload, onde seria indicado o iniciador do Open Banking na abertura de Notificação de Infração, como no exemplo abaixo:

- Fraude (fraud);
- Associada a uma solicitação de devolução (refund_request);
- Cancelamento da devolução (refund_cancelled);
- **Iniciada por Open Banking (fraud_OpB_CNPJ) – (Campo traria o CNPJ do iniciador)**



GT SEG

Pagamentos Instantâneos

Obrigado!



**BANCO CENTRAL
DO BRASIL**