

14º Fórum Pix GT SEG Pagamentos Instantâneos

Apresentação da evolução dos trabalhos de segurança do PIX



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

Ciclos de contribuições

Início das reuniões em dezembro de 2019

- ✓ 1º Ciclo – Apresentado no 07º Fórum PI – Fevereiro/20
- ✓ 2º Ciclo – Apresentado no 08º Fórum PI – Abril/20
- ✓ 3º Ciclo – Apresentação no 09º Fórum PI – Junho/20
- ✓ 4º Ciclo – Apresentação no 10º Fórum PI – Agosto/20
- ✓ 5º Ciclo – Apresentação no 11º Fórum PI – Outubro/20
- ✓ 6º Ciclo – Apresentação no 12º Fórum PI – Janeiro/21
- ✓ 7º Ciclo – Apresentação no 13º Fórum PI – Abril/21



8º Ciclo – Apresentação no 14º Fórum PI – Junho/21

Objetivos

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

Participantes*

- | | |
|-------------|-----------------------|
| 1. ABBC | 11. ZETTA |
| 2. ABECS | 12. PSTI ABBC |
| 3. ABIPAG | 13. PSTI C&M SOFTWARE |
| 4. ABO20 | 14. PSTI JD |
| 5. ABRACAM | 15. SINDTELEBRASIL |
| 6. ABRANET | 16. TESOURO NACIONAL |
| 7. AGEV | 17. B3 |
| 8. AMPEF | 18. CIP |
| 9. FEBRABAN | 19. Claro |
| 10. PAGOS | 20. RTM |

* Participantes aprovados pelo Banco Central

GT de Segurança | Contribuição sobre as mudanças no Manual de Segurança Pix

Avaliação: considerações sobre as mudanças no Manual de Segurança do Pix

Ao longo deste 8º ciclo de colaborações do GT Seg, o grupo avaliou as propostas realizadas pelo time técnico do Banco Central e contribuiu com as considerações dos especialistas participantes do GT.

❖ Considerações do GT SEG:

- ❖ Entendemos que APIs ou outros sistemas acessados por aplicativos do PSP devem implementar criptografia na comunicação, além de mecanismos de autenticação forte, de forma a garantir que **os clientes da API sejam apenas os aplicativos da instituição e impedir ataques de *man-in-the-middle*.**
- ❖ Conclui-se que a técnica a ser adotada no controle deve ser responsabilidade do PSP (prestador de serviço), mitigando desta forma os riscos apresentados, mas sugerimos manter a utilização do mTLS nas APIs de PIX, com os mecanismos atuais de Oauth2, e de forma opcional a cada PSP, a implementação de FAPI.
- ❖ Da mesma forma, reforçamos a sugestão da utilização de mTLS e do *guideline* do FAPI também no caso de aplicativos e outros softwares clientes do PSP, reforçando ainda mais a segurança do ecossistema.
- ❖ **Sugerimos a obrigatoriedade dos mecanismos de segurança para impedir** a engenharia reversa, descompilação, manipulação de código, modificação de credenciais ou parâmetros de segurança, dentre outras técnicas que resultem na sua adulteração ou comprometimento. São exemplos:
 - Android – DEXguard ou Dexprotector ou ProGuard (R8)
 - IOS - Ixguard ou Dexprotector

GT de Segurança | Agenda 9º Ciclo

Meses

Julho | Agosto | Setembro

Reuniões GT SEG – Quinzenais¹ – Quintas período da manhã

08/07

22/07

05/08

19/08

02/09

Pauta para o próximo ciclo:

1 Pix por Aproximação
Estudo: NFC (*Near Field Communication*); RFID (*Radio Frequency Identification*);
Bluetooth;

2 QR Code gerado pelo
pagador

¹Havendo necessidade será convocada reuniões extraordinárias

GT SEG

Pagamentos Instantâneos

Obrigado!

