

7º Fórum PI



**BANCO CENTRAL
DO BRASIL**

GT SEG

Pagamentos Instantâneos

Apresentação dos aspectos de segurança

São Paulo, 18 de Fevereiro de 2020

gtsegpi.febrababn@febraban.org.br

GT de Segurança I Motivadores, participantes e metodologia

Contexto

Após a instituição do GT Seg de Pagamentos Instantâneos pelo BCB, a FEBRABAN secretariou o GT convidando as associações abaixo a participar e conduzir as discussões.

Participantes

ABIPAG
ABECS
PAGOS
ABRACAM
ABBC
AGEV
AMPEF
ABRANET
ZETTA
FEBRABAN
TESOURO NACIONAL
CLARO
PSTI C&M SOFTWARE
PSTI ABBC
PSTI JD
CIP
B3

Objetivos

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

9 reuniões
Entre dez/19 e fev/20

Premissas e documento utilizados

- Documento de Especificações Técnicas e de negócios do ecossistema de pagamentos instantâneos brasileiro – versão 4.0
- Documento de especificações - fluxos de portabilidade e reivindicação
- Manual de Segurança PI – versão 1.0
- Definições detalhadas das mensagens do Catálogo de Mensagens do Sistema de Pagamentos Instantâneos (SPI) - versão 1.1
- Manual da Interface de Comunicação - versão 1.1

GT de Segurança | Agenda de discussão

Contexto

Após a instituição do GT Seg de Pagamentos Instantâneos pelo BCB, a FEBRABAN secretariou o GT convidando as associações abaixo a participar e conduzir as discussões.

Apresentaremos resultados dos trabalhos na seguinte estrutura:

1. Base centralizada de segurança
2. Fluxo de cadastramento, portabilidade e reivindicações de chave de endereçamento
3. QR code dinâmico – informações adicionais
4. Recomendações técnicas
5. Recomendações estratégicas

GT de Segurança | Agenda de discussão

Contexto

Após a instituição do GT Seg de Pagamentos Instantâneos pelo BCB, a FEBRABAN secretariou o GT convidando as associações abaixo a participar e conduzir as discussões.

Apresentaremos resultados dos trabalhos na seguinte estrutura:

1. Base centralizada de segurança
2. Fluxo de cadastramento, portabilidade e reivindicações de chave de endereçamento
3. QR code dinâmico – informações adicionais
4. Recomendações técnicas
5. Recomendações estratégicas

1. Proposta de Base Centralizada de Segurança (1/2)

Contexto

Criação de um repositório centralizado para que seja possível o armazenamento e consulta de informações relativas à segurança que possam subsidiar a escoragem de fraudes das transações.

Estudo e Proposta

- Devido o **curto tempo de análise transacional**, informações adicionais às especificadas serão importantes para garantir a segurança do ecossistema.
- **Repositório único** com essas informações adicionais será fundamental para garantir acesso ágil por parte de todos os Participantes Diretos
- As operações que utilizam a **chave de endereçamento** são as que, a princípio, apresentam maior risco de fraude
- Todas as transações interbancárias feitas através de **chave de endereçamento** e **QR Code estático** devem consultar a base.
- O DICT é a melhor solução para desempenhar o papel de armazenar e tornar disponíveis essas informações (Conforme tabela abaixo):

DICT	Prós	• Eficiência no ecossistema por ser uma base única • Reduz o risco de informações divergentes entre outras bases • Reduz o custo financeiro de criação e manutenção • Reduz o SLA das consultas tornando o sistema mais eficiente
	Contras	• Onera o processo de consulta à DICT, pois será consultada em 100% das transações interbancárias. • Maior capacidade de processamento e armazenamento
Outra Base	Prós	• Possibilidade de consultar todas as transações interbancárias (não apenas as através de chave)
	Contras	• Aumento do risco de vazamento de informações (mais bases) • Aumento do risco de dados divergentes • Criação de novos processos de consulta e atualizações • Maior custo de implementação para o ecossistema

Com a chegada do novo produto, acelera-se a importância de criação de nova Base Centralizada de Segurança que possa ser utilizada por todo o mercado para todo e qualquer tipo de transação interbancária, por isso, também recomendamos sua criação.

1. Proposta de Base Centralizada de Segurança (2/2)

Contexto

Criação de um repositório centralizado para que seja possível o armazenamento e consulta de informações relativas à segurança que possam subsidiar a escoragem de fraudes das transações.

Estudo e Proposta

Informações que o DICT deveria conter:

1.	Chave (CPF/CNPJ, Telefone ou E-mail) e respectivo CPF/CNPJ	Básicas
2.	PSP, Agência e Conta de cadastro	
3.	Data de cadastramento da chave	Críticas
4.	Data da última portabilidade/reinvindicação (campos separados)	
5.	Contador da qtde de portabilidade/reinvindicação (campos separados)	
6.	PSP Direto (caso PSP de cadastro seja Indireto)	
7.	Tipo de conta (corrente, poupança, pagamento)	
8.	Indicador de conta transacional nova: Criação nos últimos 7 dias, 30 dias, 90 dias, 180 dias, 360 dias, acima de 360 dias.	
9.	Status de utilização da Chave de Endereçamento Quantidade: 0 até 10, até 100, até 1000, mais que 1000 Período: últimos 7 dias, 30 dias, 90 dias 360 dias	
10.	Chave em processo de análise de disputa: (S/N)	
11.	Data da análise da disputa	Desejadas
12.	Data de criação do Telefone Celular	
13.	Confirmação da titularidade do Telefone	

Consulta de informações sobre o Número de Telefone

Procedimento: Sempre que houver uma solicitação de cadastro, portabilidade ou reivindicação de chave de número de celular o DICT validaria as informações do telefone celular junto as operadoras de telecom por um processo em definição com a Sindtelebrasil e ABR Telecom.

Frente de trabalho sendo conduzida em conjunto com a Sinditelebrasil e ABR Telecom

Este processo deverá evoluir com o projeto

GT de Segurança | Agenda de discussão

Contexto

Após a instituição do GT Seg de Pagamentos Instantâneos pelo BCB, a FEBRABAN secretariou o GT convidando as associações abaixo a participar e conduzir as discussões.

Apresentaremos resultados dos trabalhos na seguinte estrutura:

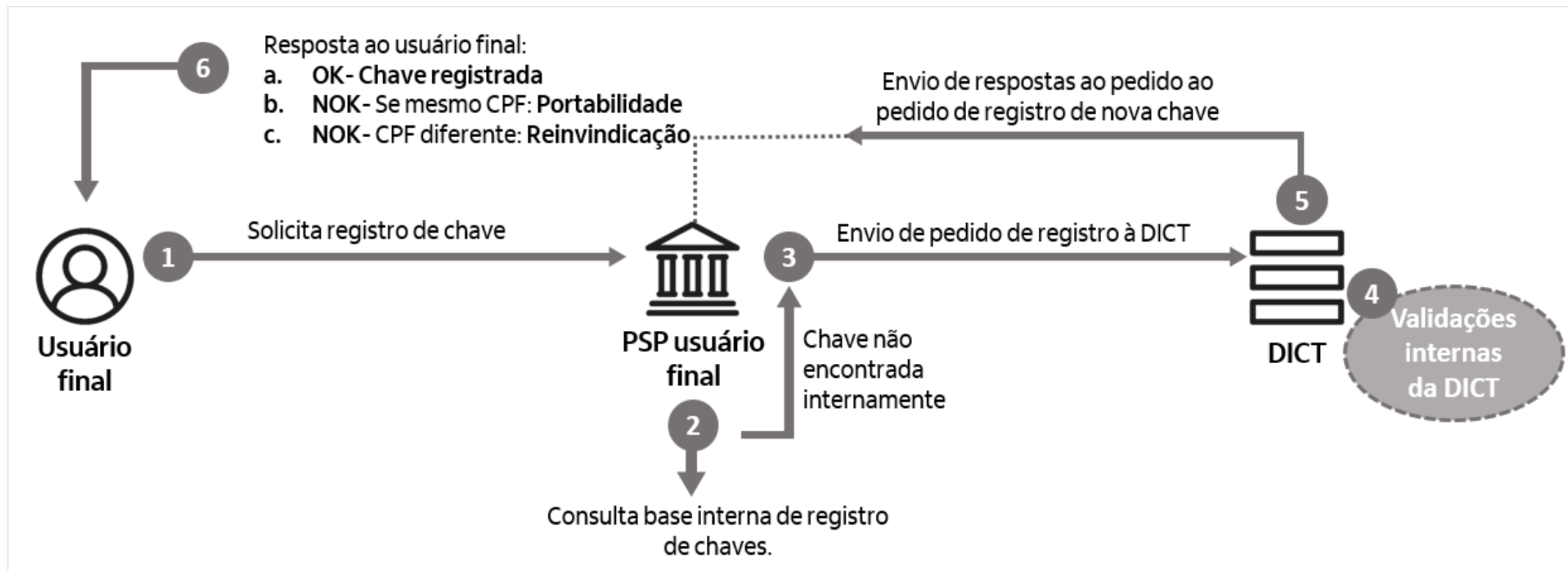
1. Base centralizada de segurança
- 2. Fluxo de cadastramento, portabilidade e reivindicações de chave de endereçamento**
3. QR code dinâmico – informações adicionais
4. Recomendações técnicas
5. Recomendações estratégicas

2. Registro, Portabilidade e Reivindicação de chaves (1/2)

Contexto

Em questionário enviado ao GT de Padronização e Requisitos técnicos foram abordados os fluxos de portabilidade e reivindicação de chaves, com o intuito de deixar o ecossistema mais fluído quando se tratando de transferências¹ de chaves de endereçamento.

Fluxo



Portabilidade: chaves já utilizadas pelo **mesmo CPF/CNPJ** em diferentes instituições.

Reivindicação: chaves já utilizadas por **outro CPF/CNPJ** em diferentes instituições.

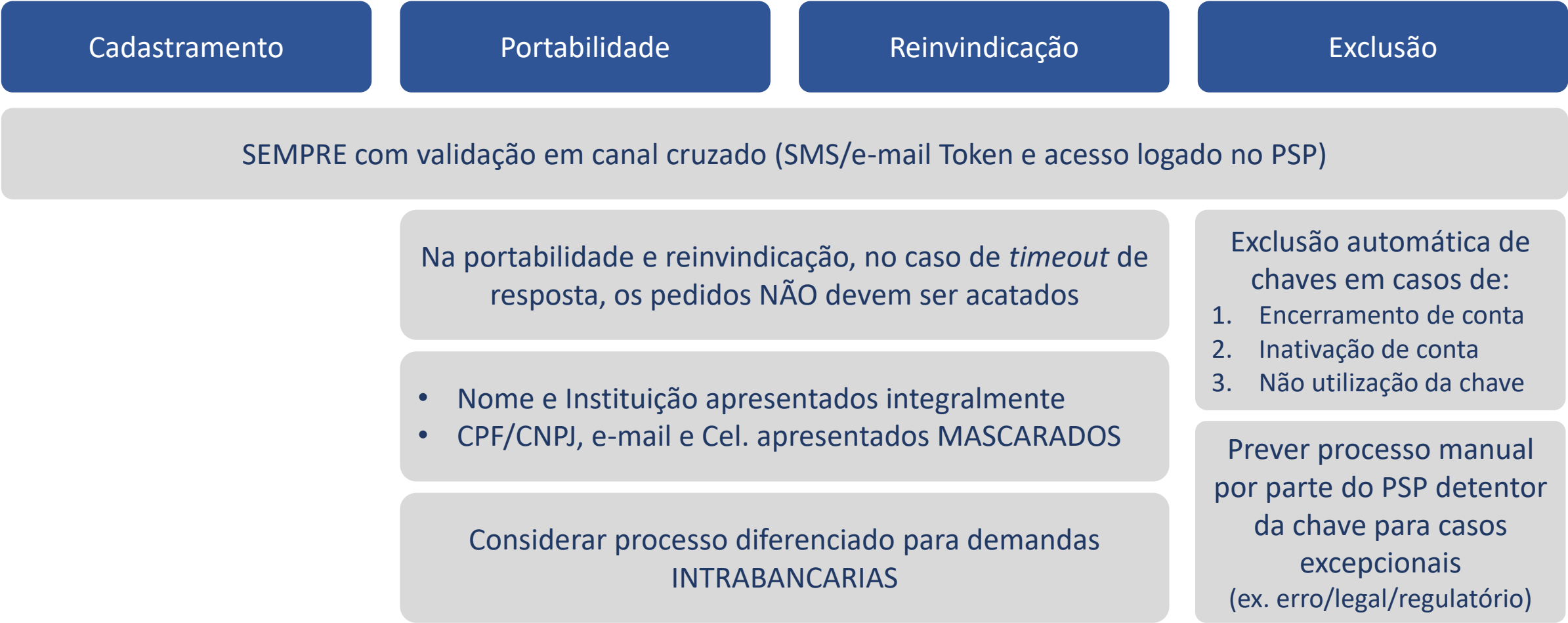
1 - a chave CPF/CNPJ não será portátil.

2. Registro, Portabilidade e Reivindicação de chaves (2/2)

Contexto

Em questionário enviado ao GT de Padronização e Requisitos técnicos foram abordados os fluxos de portabilidade e reivindicação de chaves, com o intuito de deixar o ecossistema mais fluído quando se tratando de transferências de chaves de endereçamento.

Principais alterações propostas



GT de Segurança | Agenda de discussão

Contexto

Após a instituição do GT Seg de Pagamentos Instantâneos pelo BCB, a FEBRABAN secretariou o GT convidando as associações abaixo a participar e conduzir as discussões.

Apresentaremos resultados dos trabalhos na seguinte estrutura:

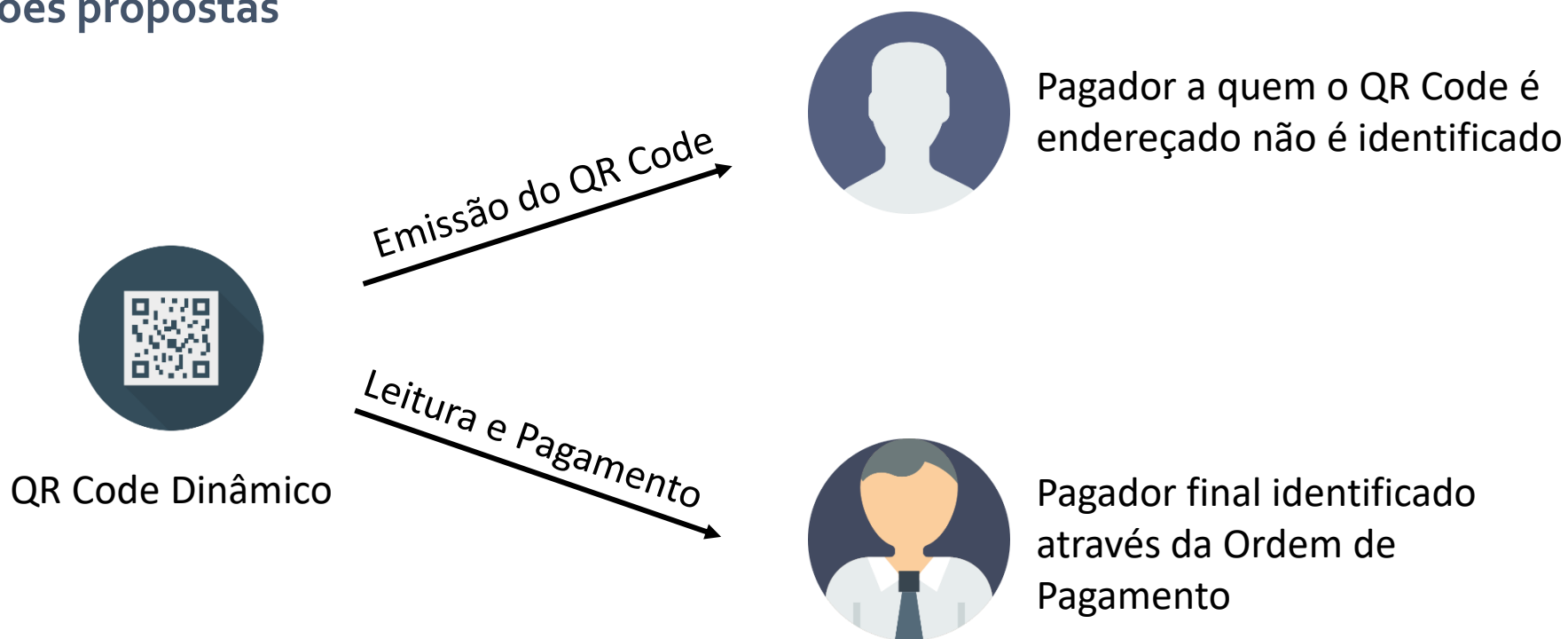
1. Base centralizada de segurança
2. Fluxo de cadastramento, portabilidade e reivindicações de chave de endereçamento
- 3. QR code dinâmico – informações adicionais**
4. Recomendações técnicas
5. Recomendações estratégicas

3. Uso do QR Code Dinâmico (1/2)

Contexto

O QR Code dinâmico não prevê o campo com a identificação do CPF/CNPJ a quem foi endereçado o pagamento. Isso pode abrir espaço para omissão de recursos, utilização de contas laranjas e desvio de finalidade.

Principais alterações propostas



Definição da existência de um campo (inicialmente) opcional no QR Code Dinâmico para identificar o pagador a quem o QR Code foi endereçado.

Campo deverá ser obrigatório no desenvolvimento da Requisição de Pagamento.

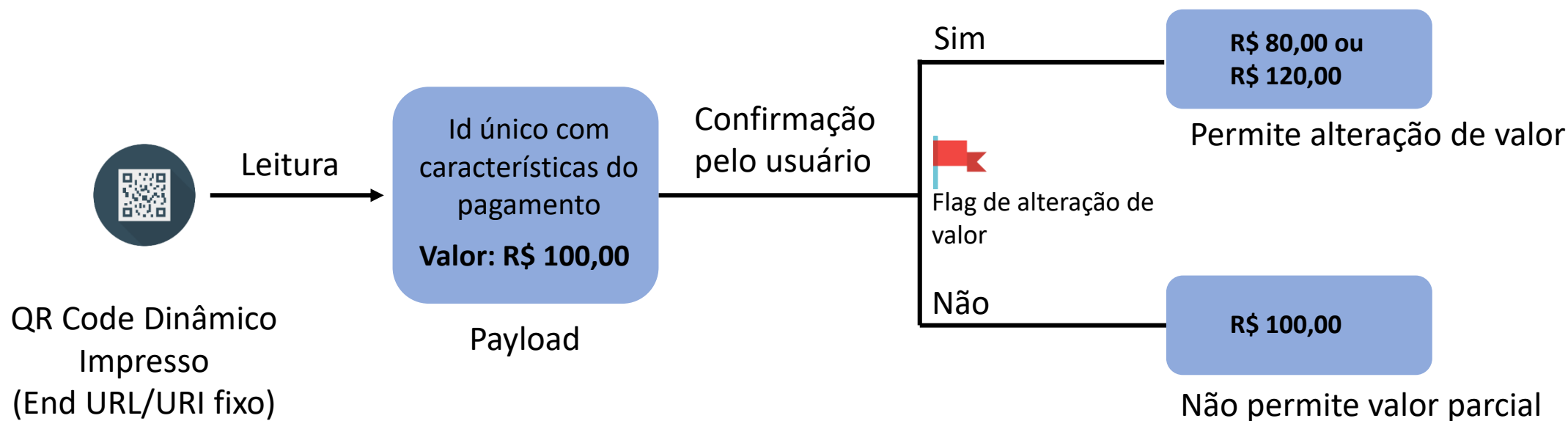
3. Uso do QR Code Dinâmico (2/2)

Contexto

No uso dos QR Codes, o dinâmico possui características de alteração de valor e identificação do pagador que devem ser abordadas para garantir a segurança e integridade do ecossistema.

Principais alterações propostas

1. Não deve ser permitida a alteração dos dados do *payload*, sem que haja alteração do campo “Identificador único na origem”.
2. Criação de FLAG no momento de emissão do QR Code para permissão (ou não) de alteração de valor no momento do pagamento.
3. Deve haver consistência de valor no momento de validação da conta recebedora pelo PSP Recebedor.
4. Criação de código de retorno específico para casos de inconsistência de valor.



Pode determinar a experiência do cliente de alteração de valor

GT de Segurança | Agenda de discussão

Contexto

Após a instituição do GT Seg de Pagamentos Instantâneos pelo BCB, a FEBRABAN secretariou o GT convidando as associações abaixo a participar e conduzir as discussões.

Apresentaremos resultados dos trabalhos na seguinte estrutura:

1. Base centralizada de segurança
2. Fluxo de cadastramento, portabilidade e reivindicações de chave de endereçamento
3. QR code dinâmico – informações adicionais
- 4. Recomendações técnicas**
5. Recomendações estratégicas

4. Recomendações Técnicas

Contexto

Com a revisão do documento “Manual de Segurança SPI” surgiram diversos pontos de recomendação, já enviados, e que demandam revisão a cada nova versão do documento.

Principais alterações propostas

CERTIFICADOS

- Mensageria específica para atualização dos certificados do Bacen;
- Detalhamento do processo de troca de certificado do BACEN;
- Definição sobre processo de verificação de revogação dos certificados BACEN;
- A documentação deve deixar claro como se dará a comunicação para a revogação antecipada dos certificados.

ASSINATURA DO JSON

- Atualização do documento de especificação técnica para definir padrão de assinatura;
- Especificações de padrões criptográficos (tipos, tamanhos de chaves e algoritmos permitidos, processos de assinatura digital etc);

LISTA DE CHAVES PÚBLICAS

- Especificação do processo de acesso e de gerenciamento das chaves públicas e da lista de domínios válidos.

GT de Segurança | Agenda de discussão

Contexto

Após a instituição do GT Seg de Pagamentos Instantâneos pelo BCB, a FEBRABAN secretariou o GT convidando as associações abaixo a participar e conduzir as discussões.

Apresentaremos resultados dos trabalhos na seguinte estrutura:

1. Base centralizada de segurança
2. Fluxo de cadastramento, portabilidade e reivindicações de chave de endereçamento
3. QR code dinâmico – informações adicionais
4. Recomendações técnicas
5. Recomendações estratégicas

5. Recomendações estratégicas (1/1)

Contexto

Ao longo das reuniões do GT Seg surgiram algumas recomendações estratégicas para manter a segurança do ecossistema.

Principais alterações propostas

Definição de papéis e responsabilidades dos participantes com relação à análise de Fraudes, colocando o **Participante Direto** como responsável por garantir a autenticidade das transações.



Fortalece a segurança do SPI, certificando que haja uma dupla conferência anti-fraude (Participante Direto e Indireto) e garante controle do Regulador perante o responsável pelas transações

Aderência da especificação para o cumprimento das obrigações dispostas na **Circular 3978**.



Garantir que todos participantes tenham informações necessárias para rastreamento do fluxo de recebimentos e pagamentos

Prever de forma clara a autonomia para os PSPs rejeitarem transações em caso de suspeitas de fraude/PLD e estabelecerem processos de autorregulação.



Autonomia para decisões importantes para garantir a segurança:

- Limites transacionais (por canal, horário, etc)
- Forma de Autenticação entre o usuário e o PSP
- Regras e processo de disputas de transações

Definição de limites de valor máximo evolutivos para as transações, conforme amadurecimento do ecossistema



Evitar fraudes de altos valores em período curto de tempo, devido a liquidez do produto, assim como ter regras claras para aceite de transações entre PSPs

GT de Segurança I Conclusão

1. Base centralizada de segurança

- Utilização do DICT como **repositório centralizado** para **armazenamento e consulta de informações relativas à segurança** que possam subsidiar a escoragem de fraudes das **transações iniciadas por Chave de Endereçamento e QR Code estático**.
- Recomenda-se, paralelamente ao projeto, a criação de Base Única de Segurança para ser utilizada por todo o mercado para qualquer tipo de transação

2. Fluxo de cadastramento, portabilidade e reivindicações de chave de endereçamento

- **Sempre** utilizar **validação em canal cruzado** (SMS/e-mail Token e acesso logado no PSP)
- Na **portabilidade e reivindicação**, no caso de **timeout** de resposta, os pedidos **não devem ser acatados**
- Exclusão automática de chaves em casos de: Encerramento de conta/ Inativação de conta / Não utilização da chave
- Prever processo manual por parte do PSP detentor da chave para casos excepcionais(ex. erro/legal/regulatório)

3. QR code dinâmico – informações adicionais

- Definição do **campo**, inicialmente **opcional**, para **identificar o pagador** a quem o QR Code foi endereçado. Campo **deverá ser obrigatório** no desenvolvimento da **Requisição de Pagamento**.
- **Criação de parâmetro**, na emissão do QR code, para a permissão ou não **de recebimento de valor diferente do original**, assim como os processos de validação relacionados.

4. Recomendações técnicas

- Com a revisão do documento “**Manual de Segurança SPI**” surgiram novos **pontos de recomendação**, já enviados, e **que demandam revisão pelo GT SEG** a cada nova versão do documento.

5. Recomendações estratégicas

- Definição de **papeis e responsabilidades dos participantes com relação à análise de Fraudes**, colocando o Participante Direto como responsável por garantir a autenticidade das transações.
- Aderência da especificação para **o cumprimento da Circular 3978**. Prever de forma clara a autonomia para os PSPs rejeitarem transações em caso de suspeitas de fraude/PLD e estabelecerem processos de autorregulação.
- Definição de **limite de valores máximos** transacionais evolutivos, **conforme o amadurecimento do ecossistema**.

5. Continuidade dos trabalhos

Consideramos ser importante a **continuidade do GT SEG por tempo indeterminado** com o intuito de avançar nas análises e frentes já iniciadas, seguindo até que haja a maturidade do ecossistema de Pagamentos Instantâneos

7º Fórum PI



**BANCO CENTRAL
DO BRASIL**

GT SEG

Pagamentos Instantâneos

Apresentação dos aspectos de segurança

São Paulo, 18 de Fevereiro de 2020

gtsegpi.febrababn@febraban.org.br