

08º Fórum PI

GT SEG Pagamentos Instantâneos

Apresentação da evolução dos trabalhos de segurança do PIX



**BANCO CENTRAL
DO BRASIL**

AGENDA

- 1. Experiência de Cadastramento, Portabilidade e Reivindicação de Chaves***
- 2. Processo de Reinvindicação de Chave***
- 3. Processo de Marcação de Suspeita de Fraudes (chave em disputa)***
- 4. Base de Prevenção a Fraudes de Mercado***
- 5. Definições relacionadas à suspeita de Fraudes e infrações a PLD***

GT de Segurança | Experiência de Cadastramento, Portabilidade e Reinvidicação

Contexto

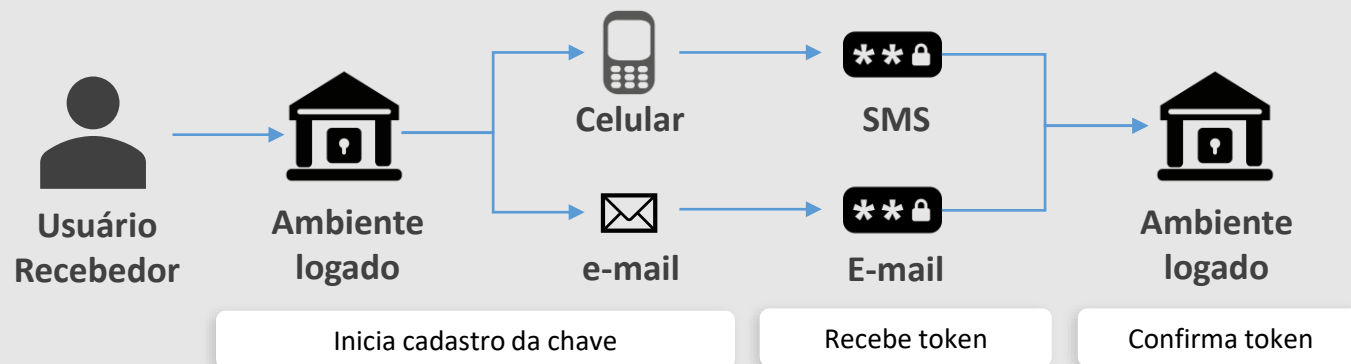
No contexto da experiência de cadastramento, portabilidade e reinvidicação de chaves de endereçamento ficou definida a validação cruzada (“tokenizada”) das chaves de e-mail e telefone celular como recomendação do Banco Central aos PSPs Recebedores.

Estudo e Proposta

Pontos de Atenção

- Fragilidade do ecossistema por PSPs não aderentes à essa recomendação
- Possibilidade de cadastramento ou portabilidade/reinvidicação sem a confirmação de posse da chave
- Aumento das tentativas de fraude e tratamento por instituições participantes gerando maior insegurança
- Fraudador procura sempre caminho mais fácil

Proposta: Processos de cadastramento, portabilidade e reinvidicação com **validação cruzada obrigatória**



- Processo altamente conhecido e disseminado no mercado digital para verificação de canais de contato em processo de *onboarding* e cobrança

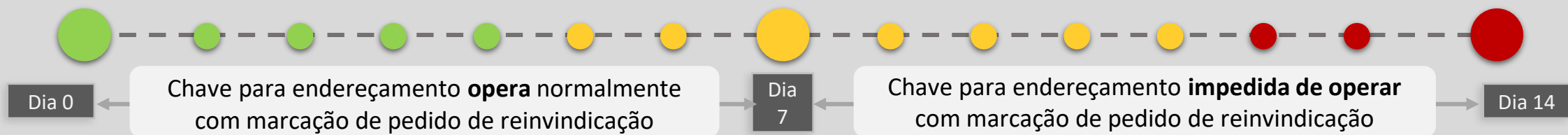
IMPORTANTE: O GT SEG ENTENDE QUE A VALIDAÇÃO CRUZADA DEVE SER OBRIGATÓRIA PARA TODOS PSPs

GT de Segurança | Processo de Reinvidicação de chave de endereçamento

Contexto

Experiência de reinvidicação solicita validação cruzada apenas no início do processo de reinvidicação com a migração automática de chaves ao final do período quando não houver atuação por parte do detentor atual da chave

Novo Processo apresentado pelo BCB

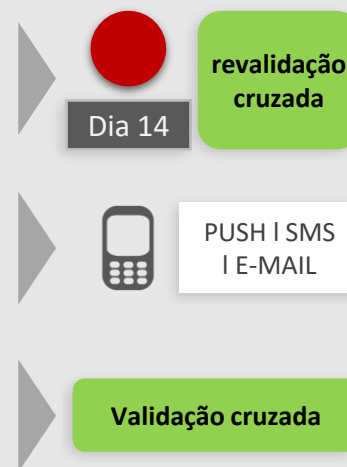


Pontos de Atenção

- Fraudador tomar a chave do cliente com apenas um acesso momentâneo da senha de e-mail ou telefone celular
- Processo de comunicação sobre portabilidade pode se tornar canal de *phishing* de informações da conta do cliente (facilita engenharia social)
- Cliente não proprietário não abrir mão da chave atual (sequestro de chave)

Propostas:

- Após o final do período de reinvidicação de 14 dias, chave é descadastrada e usuário reinvidicador deve iniciar **novo processo de cadastramento com validação cruzada**
- **Comunicação padronizada** com usuário portador atual da chave através do anexo VI – Manual de Experiência do Usuário
- Em caso do cliente detentor atual querer fazer a manutenção da chave, **comprovar posse através de validação cruzada**



Importante: No caso do usuário doador **confirmar** ou **negar** (através de validação cruzada) a reinvidicação o processo é concluído, não havendo necessidade de aguardar 14 dias

GT de Segurança | Fluxo de uso da informação de disputa

Contexto

Após posicionamento do BCB sobre informações de disputa na DICT, análises foram aprofundadas com objetivo de manter compartilhamento de informações de fraude, garantindo os seus benefícios, mas sem trazer prejuízos ao usuário recebedor

Proposta Inicial (binária)

10. Chave em processo de análise de disputa (S/N)
11. Data da análise da disputa



Nova Proposta (estatística)

- % Transações Disputadas (0-1 dia)
% Transações Disputadas (0-7 dias)
% Transações Disputadas (0-30 dias)

Sugestão de regras aplicadas à Proposta Atual:

- I. A variável “% Transações Disputadas” será calculada através da quantidade de transações com **suspeita de fraudes**, sobre a quantidade total de transações realizadas pela **chave** nos períodos de 0 a 1 dia, 0 a 7 dias e 0 a 30 dias; Ex.: a chave [aaa@gmail.com](#) abaixo realizou 2 transações em d-1, sendo que houve uma suspeita de fraude (1/2=50%), contudo, o cliente realizou 20 transações na semana (1/20=5%) e 100 no mês (1/100=1%). A chave de celular do mesmo CPF no BANCO2, onde não há fraude, não é prejudicada.
- II. A marcação de suspeita de fraude no DICT será feita à toda requisição de devolução feita pelo PSP pagador por motivo de fraude (CP76 - art. 39 - §1º - Inciso III)
- III. O BCB fará o processamento de cálculo desses campos apenas uma vez ao dia, não onerando o DICT.
- IV. PSP Recebedor tem acesso rápido às informações de fraude da chave, realizando as análises e excluindo a chave quando necessário, minimizando fraudes futuras

Exemplos:

DICT							
CHAVE	CPF	CONTA	PSP Origem	...	% Transações Disputadas (0-1 dia)	% Transações Disputadas (0-7 dias)	% Transações Disputadas (0-30 dias)
aaa@gmail.com	111.222.333-04	554488965	BANCO1	...	50%	5%	2%
(11)945426688	111.222.333-04	21566871	BANCO2	...	-	-	-
123.456.789-09	123.456.789-09	1001265469	BANCO3	...	100%	100%	100%
321.654.987-12	321.654.987-12	226598756	BANCO4	...	-	-	-

GT de Segurança | Base Centralizada de Prevenção a Fraudes

Contexto

BCB acatou o pleito de utilização do DICT para o compartilhamento de informações relativas ao risco das transações para todos os tipos de iniciação de pagamentos, com exceção da iniciação por input manual de dados bancários, e **sugeriu o desenho e a criação de base centralizada privada no mercado** para ser utilizado pelo PIX e outros meios de pagamento

Retorno para a sugestão do BCB:

GT SEG acatou a sugestão e FEBRABAN iniciará os trabalhos relativos a construção da Base de Prevenção a Fraudes paralelamente ao PIX

- FEBRABAN organizará agenda inicial junto aos times de negócios, segurança e prevenção à fraudes para desenho do projeto
- Irá secretariar com o apoio do BCB o relacionamento com entidades governamentais, empresas de telecomunicações e outras entidades que poderão aportar informações relevantes à segurança do ecossistema financeiro
- Avaliará, juntamente com outras associações interessadas, abertura de RFP com empresas habilitadas a prestar o serviço de desenvolvimento e manutenção da base, assim como realizar o desenho da solução com as premissas de garantir a sustentabilidade e baixo custo operacional da base.

GT de Segurança I Casos de Suspeita de Fraude e infração à PLD

Contexto

BCB determinará importantes limites máximos diferenciados de tempo para análises de transações com suspeita de fraude ou de infração à regulação de PLD e, em consulta pública, determinou o bloqueio do valor em conta do beneficiário enquanto a análise é feita pelo PSP Recebedor

Pleito ao BCB

Aprofundar fluxo de análise de infração a regulações de PLD e do CSNU* junto ao GT SEG, garantindo alinhamento entre especificações e resposta à Consulta Pública 76/2020

Retenção do valor no PSP Pagador

- Possibilita **análise manual**, tornando assertiva a decisão de aprova/nega a transação
- Modelo já existente para TED/DOC, mostrando-se eficaz no combate a fraude (**avaliar tempos factíveis para análise**)
- Definir **comunicação** para o cliente que iniciou pagamento

Retenção do valor no PSP Recebedor

- O processo de retenção no PSP Recebedor pode agregar no controle das resoluções relacionadas à PLD e sanções impostas pelo CSNU
- Decidir se a **análise** deve ser **pré ou pós troca de reservas**
- Decisão sobre **sensibilizar a conta do recebedor antes ou após término da análise**, assim como sua respectiva comunicação
- Definição de **casos de uso e valores mínimos** que podem ter período diferenciado para análises
- Pode haver impacto para clientes caso haja dois temporizadores.

08º Fórum PI

GT SEG Pagamentos Instantâneos



**BANCO CENTRAL
DO BRASIL**