Pagamentos Instantâneos

Especificações técnicas e de negócio do ecossistema de pagamentos instantâneos brasileiro

Anexo VII - Potenciais ameaças ao DICT e mitigadores

Versão 1.0

BANCO CENTRAL DO BRASIL

SUMÁRIO

Apresentação 3

Glossário 4

1. Registro de chaves 5

1.1. Cenários de abuso 5

1.1.1. Solicitação de registro de chave cuja posse pertence a outro usuário 5

1.1.2. Solicitação de valores após vinculação a conta laranja de chave apoderada ilegitimamente 5

1.1.3. Solicitação de valores após vinculação a conta aberta com documentos falsos ou furtados de chave apoderada ilegitimamente 6

2. Consulta de chaves 8

2.1. Cenários de abuso 8

2.1.1. Varredura de informações associadas a chaves 8

2.1.2. Vazamento de informações associadas a chaves por PSP atacado 8

3. Portabilidade 9

3.1. Cenários de abuso 10

3.1.1. Portabilidade para conta aberta com documentos furtados ou falsos 10

3.1.2. Portabilidade de chave para conta legítima de chave vinculada a conta fraudulenta 11

4. Reivindicação de posse 12

4.1. Cenários de abuso 13

4.1.1. Reivindicação de posse de chave validada ilegitimamente 13

5. Reconciliação 14

5.1. Cenários de Abuso 15

5.1.1. Acesso não autorizado a arquivos de checagem individual de chaves 15

5.1.2. Divergência entre base de dados do PSP e DICT 15

Histórico de revisão 16

Apresentação

No desenho do PIX, o uso de chaves para endereçamento é elemento fundamental, pois permitirá que pagamentos sejam feitos de forma bastante fácil. Por outro lado, essa facilidade traz também riscos de fraude contra os usuários finais. Segurança e facilidade de uso são pilares para o sucesso do arranjo, mas esses objetivos muitas vezes entram em conflito. Isso é especialmente evidente no desenho dos processos do DICT, em que se deseja dar uma boa experiência para o usuário e ao mesmo tempo protegê-lo contra fraudadores.

Pretende-se aqui analisar sistematicamente os processos e os serviços do diretório, identificando-se os riscos e as fragilidades, bem como os mecanismos de mitigação.

Glossário

Chave para endereçamento: informação relacionada ao titular de uma conta transacional, que é utilizada para obter as informações sobre o usuário recebedor e a respectiva conta transacional, a fim de facilitar o processo de iniciação do pagamento pelo usuário pagador.

Chaves não-transferíveis: chaves cujo dono não pode ser alterado. Exemplos: CPF, CNPJ, EVP.

Chaves transferíveis: chaves cujo dono pode ser legitimamente alterado. Exemplos: número de telefone celular, e-mail.

Conta transacional: conta mantida por um usuário final em um prestador de serviços de pagamento e utilizada para fins de pagamento ou de recebimento de um PIX.

Portabilidade: funcionalidade do DICT que permite ao prestador de serviços de pagamento reivindicador alterar o vínculo de uma determinada chave para endereçamento da conta transacional original para uma nova conta transacional, mantendo a chave vinculada a um mesmo CPF ou CNPJ.

Posse de chave: domínio legítimo da chave para endereçamento por uma pessoa. A posse de uma chave por uma pessoa é aferida por um mecanismo de validação de posse ou, no caso de números de identificação oficiais (CPF, CNPJ), atribuída à pessoa que a própria chave identifica.

Prestador de serviços de pagamento (PSP): instituição financeira ou instituição de pagamento que provê serviços de pagamento para um usuário final.

Reconciliação: funcionalidade que permite ao PSP verificar se sua base local de vínculos está sincronizada com a base do DICT e aplicar as correções necessárias para corrigir divergências.

Reivindicação de posse: funcionalidade do DICT que permite ao prestador de serviços de pagamento reivindicador alterar um vínculo para uma nova conta transacional associada a um novo CPF ou CNPJ.

Validação de posse: mecanismo que demonstra domínio da chave por uma pessoa que alega ser dona.

Vínculo: associação entre uma chave para endereçamento, uma conta transacional e uma pessoa (natural ou jurídica). Pessoa deve ser titular da conta transacional e deve ter posse da chave para endereçamento.

1. Registro de chaves

A pedido do cliente, uma chave pode ser vinculada a uma conta transacional. Uma conta transacional pode ter várias[1] chaves vinculadas a ela, mas cada chave só pode estar vinculada a uma única conta. Chaves do tipo CPF, CNPJ e EVP não são transferíveis e não precisam ter validação de posse ativa para serem registradas no DICT. Chaves transferíveis, como número de telefone celular e e-mail, precisam ter posse validada para serem registradas. No caso de CPF e de CNPJ, deve haver coerência com os dados cadastrais do titular da conta. Chaves do tipo EVP são geradas pelo DICT.

1.1. Cenários de abuso

1.1.1. Solicitação de registro de chave cuja posse pertence a outro usuário

É possível que um fraudador tente vincular, a uma conta pertencente a ele, uma chave de posse de outra pessoa.

1.1.1.1. MITIGADORES

1. No caso de EVP, a chave é registrada de forma aleatória pelo DICT, de forma que, por definição, não é possível registrar EVP que já esteja registrado no DICT.

2. No caso de CPF e de CNPJ, só é possível fazer o vínculo de acordo com os dados cadastrais da conta.

3. No caso de e-mail e de número de telefone celular, os usuários precisam fazer validação ativa cruzada da chave. Ou seja, após receber o código por meio da chave que se quer registrar, o usuário deve acessar o canal de atendimento de seu PSP e inserir o código recebido para fazer o vínculo da chave àquela conta transacional específica.

1.1.2. Solicitação de valores após vinculação a conta laranja de chave apoderada ilegitimamente

[1] Limites são definidos no regulamento do DICT.

É possível que um fraudador tenha uma conta laranja em um PSP. Tendo controle da conta, o fraudador poderia fazer um pedido de vinculação dessa conta a uma chave pertencente a uma pessoa. Para conseguir demonstrar a posse da chave, o fraudador poderia atacar o mecanismo de validação de posse (*SIM Swap*, sequestro de conta de e-mail) ou solicitar códigos de validação, por engenharia social, para a pessoa dona da chave. Em seguida, poderia solicitar transferências a contatos dessa pessoa, usando técnicas de manipulação psicológica (por exemplo, dizer que se trata de emergência médica).

1.1.2.1. MITIGADORES

1. Para validação de posse de número de celular, é recomendável que seja feita verificação com as operadoras de rede de telefonia se houve troca recente de chip SIM e da titularidade do número, desde que respeitados os acordos de nível de serviço referentes ao DICT.
2. É razoável esperar que o número de celular e o e-mail usados como chave pelo usuário sejam acessados por ele com frequência, permitindo que ele identifique o sequestro da chave. Nesse sentido, recomenda-se a identificação, pelos PSPs, da correspondência entre os números de celular e os e-mails utilizados como chaves e os dados informados no cadastro das instituições.
3. É recomendado ações de educação e de conscientização dos clientes para que não repassem códigos de confirmação em chamada telefônica. Mensagem enviada com código de confirmação deve lembrar que esse código não deve ser compartilhado com outras pessoas.
4. Recomenda-se que as notificações aos clientes não sejam enviadas por SMS. Caso o PSP escolha esse mecanismo de notificação, é recomendável utilização de mecanismos de autenticidade. Por exemplo, Verified SMS, na plataforma android®.
5. Na confirmação de uma transferência, aparecerá o nome do titular da conta para verificação pelo pagador. Como nesse cenário o titular é um laranja, um pagador atento observaria a divergência e não confirmaria o pagamento. Ações de educação e de conscientização de clientes para que a transação seja iniciada somente após a identificação do usuário recebedor podem ajudar a disseminar esse hábito.
6. Na avaliação de risco de um pagamento, PSP deverá considerar a data de vinculação da chave à conta e a data de abertura da conta. Essas informações serão repassadas pelo DICT ao PSP do usuário pagador quando a chave for consultada.

1.1.3. Solicitação de valores após vinculação a conta aberta com documentos falsos ou furtados de chave apoderada ilegitimamente

É possível que um fraudador abra conta em um PSP com documentos falsos ou furtados de uma vítima. O fraudador poderia então fazer um pedido de vinculação dessa conta a uma chave também pertencente à vítima. Para chaves do tipo CPF/CNPJ, a vinculação poderia ser feita sem validações adicionais. Para chaves transferíveis, o fraudador poderia atacar o mecanismo de validação de posse (SIM Swap, sequestro de conta de e-mail) ou solicitar códigos de validação, por engenharia social, à vítima. Em seguida, poderia solicitar transferências a contatos dessa pessoa, usando técnicas de manipulação psicológica. Como o titular da conta é a vítima, na confirmação de um pagamento apareceria o nome dela, dando maior credibilidade às solicitações de transferência feitas pelo fraudador.

1.1.3.1. MITIGADORES

1. Os mitigadores mencionados em 1.1.2.1 se aplicam, à exceção do mecanismo de confirmação do recebedor, que, nesse caso, mostraria o nome do titular da conta, que é também a pessoa dona da chave.

2. Consulta de chaves

2.1. Cenários de abuso

2.1.1. Varredura de informações associadas a chaves

Para permitir a confirmação de que o pagamento está sendo endereçado à pessoa certa, algumas informações pessoais do recebedor são mostradas ao pagador. Isso abre a possibilidade de abusos, pois usuários poderiam consultar informações de chaves sem confirmar pagamentos.

2.1.1.1. MITIGADORES

1. O DICT possui mecanismo de limitação da quantidade de consultas que não resultam em pagamentos liquidados que um usuário pode fazer. Esse limite impede que um usuário obtenha informações em escala.
2. PSP deve manter mecanismo limitador equivalente para consultas à sua base de endereçamento, usada no cenário de *booktransfer*.
3. PSP deve manter mecanismos de detecção de abusos por parte de usuários, podendo vir a suspender serviços em caso de violação dos termos de uso.
4. A única potencial informação sensível, que é o CPF do usuário recebedor, será apresentado de forma mascarada.

2.1.2. Vazamento de informações associadas a chaves por PSP atacado

Um PSP poderia vir a sofrer um ataque e as informações de chaves de todos PSPs poderiam vazar, por meio de requisições forjadas ao DICT.

2.1.2.1. MITIGADORES

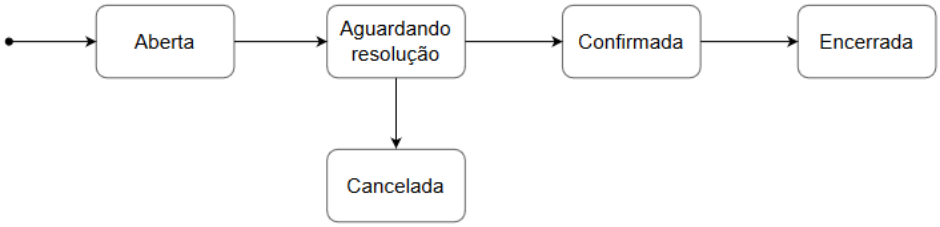
1. O DICT possui mecanismo de limitação da quantidade de consultas que não resultam em pagamentos liquidados que um PSP pode fazer. Esse limite retardaria um vazamento completo dos dados do DICT.

3. Portabilidade

Na portabilidade, o cliente deseja mudar a vinculação de uma chave sua para uma conta em outro PSP. Todos os tipos de chave podem ser portados, exceto EVP.

De forma resumida, o processo de portabilidade ocorre da seguinte forma:

1. A pedido do cliente, PSP reivindicador cria um pedido de portabilidade. DICT altera estado da portabilidade para “Aberta”.
2. PSP doador recebe o pedido de portabilidade. DICT altera estado da portabilidade para “Aguardando resolução”.
3. Cliente é direcionado ao canal do PSP doador e confirma portabilidade. Após confirmação, chave deixa de estar vinculada à conta no PSP doador. DICT altera estado da portabilidade para “Confirmada”.
4. PSP reivindicador, ao observar mudança para estado “Confirmada”, encerra portabilidade. Chave passa a estar vinculada à conta no PSP reivindicador. DICT altera estado da portabilidade para “Encerrada”.



Destacam-se os seguintes elementos no desenho:

1. Processo se inicia com pedido do cliente no PSP de destino da portabilidade (reivindicador).
2. É necessária confirmação da portabilidade pelo cliente no PSP doador.
3. Ao final do prazo máximo de resolução[2], não havendo confirmação pelo cliente, portabilidade deve ser cancelada pelo PSP doador.

[2] Prazo está definido no regulamento do DICT.

4. Enquanto não estiver confirmada ou encerrada, portabilidade pode ser cancelada tanto pelo PSP doador quanto pelo PSP reivindicador, somente a pedido do cliente ou em caso de suspeita de fraude.

3.1. Cenários de abuso

3.1.1. Portabilidade para conta aberta com documentos furtados ou falsos

É possível que um fraudador abra conta em um PSP com documentos falsos ou furtados de uma vítima. Tendo controle dessa conta, o fraudador poderia então fazer um pedido de portabilidade de uma chave pertencente à vítima. Sendo a portabilidade bem-sucedida, pagamentos endereçados a essa chave passariam a ser creditados na conta fraudulenta. O mecanismo de confirmação do recebedor pelo pagador no momento do pagamento não seria efetivo, pois apareceria o nome da pessoa para a qual se pretende fazer o pagamento.

Considerando o cenário em que um fraudador obteve sucesso na abertura de conta com documentos da vítima, o processo de portabilidade poderia ser abusado das seguintes maneiras:

3.1.1.1. ATAQUE NO MECANISMO DE VALIDAÇÃO DE POSSE DE CHAVE TRANSFERÍVEL

Antes de fazer o pedido de portabilidade, o PSP reivindicador deve fazer a validação da posse da chave pelo cliente, no caso de chaves transferíveis. O atacante pode fraudar a validação de posse da chave. Para números de celular, o atacante pode clonar o número de celular (SIM Swap) e assim receber códigos de confirmação enviados por SMS. Para e-mail, o atacante pode obter acesso à conta de e-mail da vítima. Tendo sido feita validação ilegítima da posse da chave, atacante conseguiria solicitar a portabilidade da chave para vinculá-la à conta fraudulenta sob seu controle.

Mitigadores

1. Para que a portabilidade seja processada, é exigida a confirmação pelo cliente no PSP doador. Atacante precisaria ter acesso ao canal de atendimento do PSP doador ou convencer a vítima a fazer a confirmação.
2. Para validação de posse de número de celular, é recomendável que seja feita verificação com as operadoras de rede de telefonia se houve troca recente de chip SIM, desde que sejam respeitados os acordos de nível de serviço do DICT.
3. O PSP doador deve enviar por canais adicionais notificação ao cliente de que uma portabilidade foi solicitada, pelo app de celular, por exemplo.

4. É razoável esperar que o número de celular e o e-mail usados como chave pelo usuário sejam acessados por ele com frequência, permitindo que ele identifique o sequestro da chave. Nesse sentido, recomenda-se a identificação, pelos PSPs, da correspondência entre os números de celular e os e-mails utilizados como chaves e os dados informados no cadastro das instituições.

3.1.1.2. ATAQUE DE PHISHING CONTRA CLIENTE NA VALIDAÇÃO DE POSSE DE CHAVE TRANSFERÍVEL

Uma alternativa ao atacante é ludibriar o cliente. O atacante poderia se passar pelo atendimento do PSP e pedir ao cliente que ele informe o código de confirmação usado para validação de posse que foi enviado por SMS ou e-mail. O atacante conseguiria, assim, validar a posse da chave e prosseguir com a solicitação de portabilidade.

Mitigadores

1. A validade de um código de confirmação deve ser a mais curta possível (poucos minutos), pois isso dificulta o ataque.
2. Para que a portabilidade seja processada, é exigida a confirmação pelo cliente no PSP doador. Isso significa que o atacante precisaria convencer o cliente também a fazer essa confirmação.
3. É recomendável ações de educação e de conscientização dos clientes para que não repassem códigos de confirmação em chamada telefônica. Mensagem enviada com código de confirmação deve lembrar que esse código não deve ser compartilhado com outras pessoas.
4. Para notificações enviadas por SMS, é recomendável utilização de mecanismos de autenticidade. Por exemplo, *Verified SMS*, na plataforma android®.

3.1.2. Portabilidade de chave para conta legítima de chave vinculada a conta fraudulenta

É possível que um fraudador abra conta em um PSP com documentos falsos ou furtados de uma vítima. Tendo controle dessa conta, pode vincular uma chave da vítima (CPF/CNPJ ou número de celular clonado) a essa conta. Nesse cenário, quando a vítima fosse tentar vincular uma chave sua a uma conta legítima sua, estaria impossibilitado de fazê-lo. Além disso, pagamentos endereçados à vítima seriam creditados na conta do fraudador.

3.1.2.1. MITIGADORES

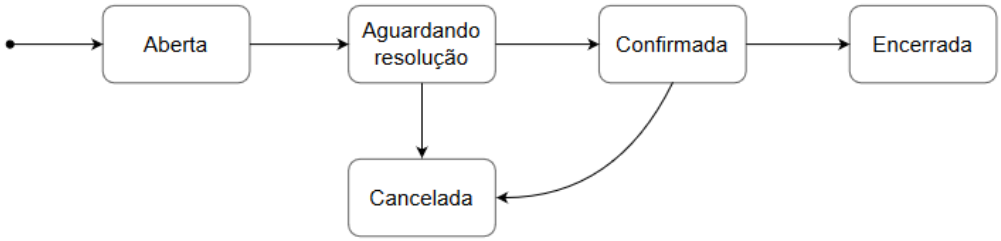
1. A consulta a uma chave no DICT retornará informação da data de abertura da conta transacional. Esse dado deverá ser considerado na avaliação de risco de um pagamento.

4. Reivindicação de posse

Na reivindicação de posse, o cliente deseja vincular uma chave que pertencia a outra pessoa, mas que permanece indevidamente vinculada à conta do antigo possuidor. O processo de reivindicação se aplica apenas a chaves transferíveis (número de celular e e-mail). Chaves como CPF/CNPJ não podem trocar de dono. Logo, não faz sentido que exista reivindicação de posse para elas. Não existe também reivindicação de posse para EVP.

De forma resumida, o processo de reivindicação de posse ocorre da seguinte forma:

1. A pedido do cliente, PSP reivindicador cria um pedido de reivindicação de posse. DICT altera estado da reivindicação para “Aberta”.
2. PSP doador recebe a reivindicação. DICT altera o estado da reivindicação para “Aguardando resolução”.
3. Durante período de resolução e período de encerramento[3], PSP doador tenta contato com cliente que terá a chave desvinculada, a fim de verificar a possibilidade de que esteja ocorrendo uma reivindicação de posse ilegítima.
4. PSP doador, ao final do prazo de resolução, não havendo indícios de fraude, deverá confirmar a reivindicação. Chave deixa de estar vinculada à conta no PSP doador. DICT altera estado da reivindicação para “Confirmada”.
5. PSP reivindicador encerra reivindicação, ao final do prazo de encerramento. Chave passa a estar vinculada à conta no PSP reivindicador. DICT altera estado da reivindicação para “Encerrada”.



[3] Prazos definidos no regulamento do DICT.

Destacam-se os seguintes elementos no desenho:

1. Processo se inicia com pedido do cliente no PSP reivindicador, onde está a conta à qual ele deseja vincular a chave.
2. Na ausência de indícios de fraude, após a passagem do prazo de resolução, o padrão é que a reivindicação seja confirmada.
3. Após confirmação da reivindicação pelo PSP doador, a chave permanecerá por um tempo (prazo de encerramento) sem vínculo algum.
4. Enquanto não estiver encerrada, a reivindicação de posse pode ser cancelada tanto pelo PSP doador quanto pelo PSP reivindicador, em caso de suspeita de fraude. Cancelamento a pedido do cliente, somente pelo PSP reivindicador.

4.1. Cenários de abuso

4.1.1. Reivindicação de posse de chave validada ilegitimamente

É possível que um fraudador abra uma conta transacional e faça uma reivindicação de posse de uma chave que pertence a uma vítima e está vinculada a uma conta dela. Para que o fraudador consiga fazer essa reivindicação, precisará antes fazer a validação de posse da chave da vítima junto ao PSP onde está a conta do fraudador. Essa validação de posse ilegítima poderia ser obtida atacando-se o mecanismo de validação (ex: SIM Swap, ou roubo de credenciais de e-mail) ou por meio de *phishing* contra o dono legítimo da chave.

Considerando o cenário em que o fraudador conseguiu criar uma reivindicação de posse de uma chave que não lhe pertence, o processo de reivindicação poderia falhar das seguintes maneiras:

4.1.1.1. PSP DOADOR, NA TENTATIVA DE CONTATAR CLIENTE, ACABA CONTATANDO FRAUDADOR

Caso o fraudador tenha clonado o número de telefone ou tenha acesso à conta de e-mail da vítima para fazer a validação de posse da chave, a comunicação do PSP doador com a vítima pelo canal da própria chave estaria comprometida. Fraudador poderia confirmar ao PSP doador que de fato é o novo dono da chave e que solicitou reivindicação dela.

Mitigadores

1. É recomendável que o PSP mantenha canal de contato adicional, distinto da chave. Por exemplo, outro número de telefone ou outro e-mail.

2. Caso PSP venha a se comunicar pelo canal da própria chave, é recomendável adotar medidas adicionais de verificação da identidade da pessoa.
3. Na avaliação do risco de fraude de uma reivindicação de posse, PSP doador deverá considerar o perfil de uso da chave e da conta vinculada.
4. O PSP doador deve enviar por canais adicionais notificação ao cliente de que uma reivindicação de posse foi solicitada, pelo app de celular, por exemplo.

4.1.1.2. VÍTIMA NÃO RECEBE NOTIFICAÇÃO DE QUE HÁ REIVINDICAÇÃO PARA UMA CHAVE QUE É SUA

É possível que a vítima não receba a notificação de que foi aberta reivindicação para chave que lhe pertence (está em viagem, por exemplo). Assim, não perceberia que está sendo vítima de uma fraude.

Mitigadores

1. Na avaliação do risco de fraude de uma reivindicação de posse, PSP doador deverá considerar o perfil de uso da chave e da conta vinculada.
2. Passado o período de resolução da reivindicação, haverá o período de encerramento. Nesse período, a chave reivindicada deixará de estar vinculada à conta da vítima, mas ainda não estará vinculada à conta do fraudador. Assim, pagamentos endereçados à vítima por essa chave no período de encerramento não serão efetivados. A falta de efetivação dos pagamentos seria um alerta adicional para que o cliente tome ação junto ao seu PSP.

5. Reconciliação

O processo de reconciliação permite ao PSP checar se os dados dos vínculos de sua base local estão iguais aos respectivos dados na base do DICT. Para isso, o PSP tem acesso a três funcionalidades na API do DICT:

1. Checagem agregada
2. Checagem individual das chaves
3. Correção de chave divergente

Durante a checagem agregada, o PSP envia um *hash* de todos os CIDs (identificador de conteúdo do vínculo) de sua base relacionados a um determinado tipo de chave, ordenados de forma crescente. O DICT então retorna *OK* ou *NOK* (*not OK*), após aplicar a mesma função *hash* sobre sua própria base.

Havendo divergência, o PSP deve realizar a checagem individual das chaves, solicitando um arquivo com os CIDs. A partir desse arquivo, o PSP pode verificar quais registros estão divergentes entre PSP e DICT.

Identificado os pontos de divergência, o PSP deve iniciar o processo de correção de chaves divergentes. Para isso, o PSP solicita a remoção de chaves que estão no DICT e não estão na sua base, bem como a adição de chaves que o DICT não possui.

5.1. Cenários de Abuso

5.1.1. Acesso não autorizado a arquivos de checagem individual de chaves

Os arquivos de checagem individual de chaves para reconciliação são gerados pelo DICT a pedido do participante. Depois de gerados, esses arquivos precisam ser armazenados e entregues ao participante solicitante. É possível que, por falhas de segurança no armazenamento ou na distribuição desses arquivos, um atacante consiga acesso a eles.

5.1.1.1. MITIGADORES

O arquivo gerado conterá apenas uma lista de CIDs (identificadores de conteúdo), que identificam inequivocamente uma chave e todos os dados associados a ela. O conhecimento do CID não permite dedução dos dados ao qual ele se refere.

5.1.2. Divergência entre base de dados do PSP e DICT

Divergências entre as bases dos PSPs e o DICT podem gerar pagamentos endereçados incorretamente.

5.1.2.1. MITIGADORES

Recomenda-se que o processo de reconciliação seja realizado diariamente, a fim de evitar que divergências permaneçam por muito tempo.

Histórico de revisão

Data	Versão	Descrição das alterações
7/4/2020	1.0	