



Análise da Labrys sobre Pix Automático (Manual PIP) (versão revisada)

I. O que mudou e porque isso importa?

O documento posto em consulta é uma nova versão do Manual de Padrões para Iniciação do Pix (v.2.7). As grandes mudanças postas em consulta são três:

1. A criação da iniciação de Pix via QR Code Composto, que é aquele que contém uma URL específica para autorização do Pix Automático.
2. A inclusão do Pix Automático como forma de iniciação de Pix, com a descrição de casos de uso, definição do padrão técnico e mapeamento para a mensagens ISO 20022
3. A atualização da API Pix para receber a funcionalidade do Pix Automático.

Nossa avaliação geral é que o design técnico e regras divulgadas até aqui para o Pix Automático vão na contra-mão das características que fizeram o Pix ser um sucesso até hoje. Ele mina importantes propriedades do design de lançamento do Pix, como sua ubiquidade, flexibilidade, evolutibilidade, extensibilidade sem alteração da infraestrutura, adaptabilidade, idempotência, segurança e minimização de dados. Ao contrário do design original do Pix, o Pix Automático: (i) não usa a funcionalidade das Chaves Pix, (ii) não adota um design flexível e evoluível, (iii) não se propõe a ser aberto para todos os usuários nem abarcar todos os casos de uso, (iv) não é focado na experiência pelo telefone celular, e (v) ao invés de seguir o conceito de plataforma sobre a qual PSPs podem criar experiências competitivas ou blocos de funcionalidade que possam ser combinados de formas flexíveis, define as jornadas específicas e rígidas que podem ser implementadas pelos participantes.

A seguir faremos uma análise sobre (1) decisões de negócio sobre o Pix Automático para, na sequência, (2) entrar nos comentários específicos ao MPI posto em consulta.

II. Nota prévia: funcionamento geral do Pix Automático e decisões de negócio tomadas até aqui

Premissa: Tal como está desenhado, o Pix Automático:

- Será exclusivo para clientes recebedores PJ;
- Obrigatório para PSPs pagadores, mas voluntário para PSPs de recebedores. Ou seja: apenas os clientes dos PSPs que optarem por oferecer a funcionalidade poderão se habilitar para receber pagamentos, mas essas empresas poderão enviar Pix Automático para qualquer usuário pagador;
- Dependerá do PSP Recebedor avaliar e aceitar o risco de assumir as perdas em caso de o usuário recebedor enviar cobranças de forma fraudulenta ao usuário pagador;
- Permitirá cobrança de valores variáveis por meio da autorização de um valor máximo de cobrança, mas não haverá um mecanismo para pedir ao usuário pagador a autorização de uma cobrança em valor superior. O envio de cobranças em valores superiores será negada;
- Somente estará disponível via API ou sistema de arquivo, o que demanda a intervenção de um intermediário, como um ERP. Não está especificada para uma experiência direta na interface do PSP Recebedor nem muito menos em seus aplicativos para dispositivo móvel;
- Somente será admitido dentro das quatro jornadas desenhadas pelo Banco Central, limitando as oportunidades para inovação e evolução do padrão sem uma nova alteração da especificação técnica e da infraestrutura de todos os participantes;
- Somente permite transferências com periodicidade bem definida (semanal, mensal, trimestral, semestral e anual);
- Não permitirá que o usuário pagador transfira as autorizações de Pix Automático de uma conta para outra caso deseje mudar de PSP.
- Não permitirá que o usuário pagador decida se quer antecipar o pagamento da cobrança automática nem prevê que o usuário pagador possa decidir sobre o débito automático após o vencimento da cobrança, com eventuais multas e juros, nos casos em que o pagamento na data do vencimento falhar.

Análise: A posição da Labrys sobre esses pontos é a que segue:

- A funcionalidade deveria estar disponível para todos os usuários, PJ e PF, e ser capaz de oferecer uma experiência segura *by design* para todos. Limitar o acesso a funcionalidades

nunca é um bom substituto à criação de balizas efetivas para o seu uso seguro. Esse tipo de estratégia apenas exclui casos de uso sem alcançar o objetivo de segurança;

- Deveria ser permitido ao usuário pagador *opt out* da funcionalidade e bloquear qualquer pedido de autorização, assim como ter a opção de bloquear pedidos de autorização de usuários recebedores específicos (block list) ou de autorizar o recebimento de pedidos de autorização de usuários recebedores específicos (allow list). Da mesma forma, o usuário pagador deveria poder controlar as cobranças recebidas, autorizando, cancelando, ou antecipando os pagamentos que desejar;
- A funcionalidade deveria ser de implementação obrigatória, inclusive nos canais de atendimento móvel (app) e web (internet banking). Assim como a funcionalidade de gerar QR Code Dinâmico também deveria. A falta de obrigatoriedade do uso das ferramentas mais flexíveis do Pix restringe a evolução do arranjo para os casos de uso que demandam mais flexibilidade, como é o caso do pagamento no comércio, que largamente ainda depende dos arranjos do cartão. A obrigação de utilizar API Pix para acesso a determinadas funcionalidades encarece e retarda a adoção do Pix e a criação de formas inovadoras de utilizar a flexibilidade que o arranjo traz em si. Uma das grandes características do Pix é que "as transações podem ser iniciadas por meio do telefone celular sem a necessidade de qualquer outro instrumento". Impor a participação de um intermediário para a criação de Pix Automático (e de QR Code Dinâmico, diga-se) dificulta a adoção dessas funcionalidades por micro, pequenas e médias empresas, como a dona da floricultura que poderia criar uma assinatura semanal de flores diretamente pelo aplicativo do seu banco, o micro produtor que faz entregas recorrentes para um mercado de produtos locais, ou a lavanderia de bairro que poderia enviar uma única cobrança mensal com o valor total gasto no mês. A importância da democratização dessa funcionalidade é ainda maior quando se considera o seu potencial de facilitar o acesso a crédito, em razão da estruturação de recebíveis fora do arranjo de cartão;
- A definição de um limite máximo de pagamento automático autorizado sem um mecanismo de autorização de eventuais transações em valor superior cria um grau de incerteza com o uso da funcionalidade. O envio de valores acima do valor máximo autorizado irá criar um risco de não-pagamento, até porque o usuário pagador teria a expectativa de que a conta seria paga e não foi. A reação natural será que os usuários recebedores enviem pedidos de autorização em valores acima da média do que esperam cobrar, aumentando a exposição dos usuários pagadores. Melhor seria permitir um mecanismo semelhante ao challenge-response quando a cobrança enviada superar o valor máximo autorizado. Nesse caso, o usuário pagador seria provocado a revisar a cobrança recebida para autorizar ou recusar o pagamento a maior;

- A limitação dos casos de uso pela definição rígida das jornadas possíveis e das periodicidades admitidas fecha o Pix Automático para inovação. Esse enrijecimento se deu tanto pela definição das quatro jornadas possíveis no próprio Regulamento do Pix quanto na arquitetura dessas jornadas no código do Pix Automático por meio das especificações técnicas que estão agora em debate. Resultado imediato dessa abordagem é que para fazer qualquer mudança na experiência ou mecanismos do Pix Automático dependerá de uma reformulação da arquitetura do Pix e do tombamento de código de todos os mais de 900 participantes. Além disso, o design da especificação e a implementação por cada participante fica mais complexa e sujeita a falha. Por fim, o espaço para o surgimento orgânico de novos casos de uso e novas maneiras de melhorar a experiência dos usuários finais se reduz muito. Preferível seria adotar um design em que blocos de funcionalidade podem ser combinados de formas arbitrárias para criar experiências diferenciadas. A Labrys apresentou uma proposta de design que permitiria essa abertura para inovação, disponível [aqui](#). Um resumo de alguns conceitos principais está disponível abaixo;
- A ausência de previsão no design de mecanismos de portabilidade das autorizações de pagamento, tanto do ponto de vista do usuário pagador quanto do usuário recebedor pode aumentar consideravelmente o custo de troca de PSP. Afinal, uma vez que todos os gastos recorrentes estão configurados em uma conta, a perspectiva de ter que voltar a registrar tudo em uma nova conta pode ser razão suficiente para permanecer no mesmo banco. Da mesma forma, não havendo uma forma nativa do arranjo para tombar autorizações de cobrança de um PSP para outro, usuários recebedores podem se sentir muito inseguros para mudar de PSP e correr o risco de perder autorizações de pagamento. Nesse caso, como o usuário pagador tinha a expectativa de que já havia autorizado as transações automáticas, o risco de não pagamento, incorrência de multas e processos judiciais não é desprezível e poderia inibir a troca de PSP, prejudicando a concorrência no mercado.
- O usuário pagador deve ter sempre a escolha sobre se, quando e como sua conta deve ser movimentada. Isso quer dizer que o usuário pagador deveria ter a opção de: (1) *opt out* do Pix Automático (isto é: determinar que seu PSP rejeite automaticamente qualquer pedido de autorização em seu nome — Rec ou SoliciRec), (2) bloquear determinados usuários recebedores (CNPJs/CPFs) de enviar solicitações de autorização (block list), (3) autorizar o recebimento de solicitações de autorização apenas de usuários recebedores pre-cadastrados (allow list), (4) antecipar cobranças já ativas, (5) autorizar ou rejeitar o pagamento de cobranças após o vencimento, e (6) autorizar ou recusar a liquidação pontual de uma cobrança acima do valor máximo autorizado.

III. Análise do documento em consulta

Comentários gerais de escolha de design da versão do MPI colocada em consulta:

III.1. O Pix Automático não deveria ser uma especificação à parte do Pix

Premissa: A consulta propõe a criação de um novo link URL com seu próprio payload de retorno com informações sobre a recorrência, a criação de uma nova espécie de QR Code e uma nova categoria de mensagem de cobrança (COBR). Além disso, a consulta deixa de lado a funcionalidade da Chave Pix para voltar a exigir informações completas como ISBN do PSP e dados bancários completos.

Análise: A consequência dessa abordagem é maior trabalho de especificação para o regulador, e de interpretação, implementação e manutenção por cada participante do arranjo, além de um maior risco de erros e inconsistências nos códigos. A versão do MPI compartilhada não trabalha com as abstrações presentes no design central do Pix. Isto é: que qualquer serviço de pagamento pode ser reduzido ao conceito de movimentação de fundos com metadados. Consequência disso é que, para que qualquer solução de pagamento seja viável, são necessários dois elementos principais: (1) uma câmara de liquidação que resolva a movimentação dos fundos (SPI) e (2) um canal de comunicação que permita a troca dos metadados relevantes entre os PSPs dos usuários (tanto na direção pagador-recebedor quanto na direção receptor-pagador).

O fluxo de liquidação diz com as regras para movimentação de fundos e é comum a qualquer produto de pagamento. Já o canal de comunicação foi resolvido no Pix por meio das mensagens trafegadas pela ICOM e pela URL do QR Code Dinâmico. São os dois caminhos que permitem a troca de dados entre o PSP Pagador e o PSP Receptor. A ICOM opera como o canal de comunicação que conecta quaisquer dois participantes do Pix. É o que confere ao arranjo o super-poder de absorver a complexidade de comunicação de qualquer produto de pagamento. Isso porque, ao invés de criar novas redes com integrações próprias de n-para-n, a ICOM centraliza e padroniza as trocas de mensagem. Assim, garante que uma única integração com a ICOM permite qualquer PSP se comunicar com todos os outros PSPs no Brasil. Para complementar esse canal geral, a mecânica do link do QR Code Dinâmico é extremamente flexível, estabelecendo um canal direto entre PSP Pagador e PSP Receptor e permitindo inclusive que um participante crie novos campos no payload de resposta que não estão na especificação técnica.

Essa é a abstração, a essência básica de qualquer sistema de pagamento sobre a qual é possível modelar qualquer funcionalidade futura, inclusive o Pix Automático. Assim, não faz sentido criar um novo canal de comunicação por meio de um novo link específico para recorrência quando já existe um meio para tal, por meio do link URL do QR Code Dinâmico. Tampouco faz sentido criar uma nova classificação de QR Code, quando a informação sobre a

recorrência pode ser retornada diretamente no payload de resposta do QR Code Dinâmico após o usuário pagador fazer a leitura da imagem e o app do seu PSP acessar o link URL. Até porque, não está claro o que deve acontecer caso, em havendo dois links, um deles não retornar o payload esperado. Assim, deveria ser mantida a classificação original de QR Codes quanto à variabilidade de seu conteúdo: o QR Code Estático é o modelo mais simples em que se inclui uma Chave Pix e um valor pre-definidos (ainda que seja 0) e o QR Code Dinâmico contém um link que permite ao PSP Recebedor incluir metadados mais complexos no payload de retorno, assim como atualizar o payload conforme a necessidade, inclusive para retornar status gone se o pagamento já foi feito ou já não está disponível. A funcionalidade do Pix Automático demanda a troca de metadados mais detalhados, pelo que pertence ao modelo do QR Code Dinâmico. Não há porque tornar o design do sistema mais complexo para permitir um QR Code Estático com link para trazer metadados adicionais. Esse é todo o propósito de se criar a figura de um QR Code Dinâmico.

Tampouco seria justificado criar uma nova forma de cobrança se a única novidade na cobrança do Pix Automático é que está vinculada a um ID de autorização. Trata-se de um campo adicional nos metadados da transação. Assim, não há por que criar uma nova especificação que repete em grande parte os dados das demais formas de cobrança para fazer esse acréscimo.

Da mesma forma, a especificação técnica do Pix até aqui fez um bom trabalho em abstrair o conceito de conta bancária ao usar a figura da Chave Pix em todas os padrões para iniciação do Pix já implementados. A proposta de MPI apresentada à consulta, contudo, volta a trabalhar com ISBNs e dados completos de conta, o que vai contra as escolhas originais de design do Pix, engessa esse pedaço do arranjo à evolução que pode ocorrer com o uso das Chaves Pix e inviabiliza importantes funcionalidades características das Chaves Pix, como por exemplo a portabilidade e redução do custo de troca de PSP. Ainda que o manual fale na possibilidade de mudança de PSP do recebedor em razão de não se vincular uma autorização a uma conta específica, o fato é que não usar Chaves Pix faz com que seja impraticável que o usuário pagador migre as autorização de Pix Automático de um PSP para outro, aumentando o custo de troca de PSP.

Assim, a especificação técnica deveria se apoiar na flexibilidade do Pix para adicionar novas funcionalidades ao invés de construir uma especificação técnica à parte para o Pix Automático. A literatura especializada reconhece as vantagens de se trabalhar com abstrações ao invés de se especificar repetidamente cada tipo de comportamento de um sistema diretamente no código. Confira-se o seguinte trecho do livro Software Abstractions: Logic, Language, and Analysis, do professor de computação no MIT, Daniel Jackson (tradução livre).

Software é construído sobre abstrações. Escolha as certas, e a programação fluirá naturalmente do design; os módulos terão interfaces pequenas e simples; e novas funcionalidades provavelmente se encaixarão sem uma extensa reorganização. Escolha as erradas, e a programação será uma série de surpresas desagradáveis: as interfaces se tornarão barrocas e desajeitadas à medida que são forçadas a acomodar interações imprevistas, e até as mudanças mais simples serão difíceis de fazer. Nenhuma quantidade de refatoração, exceto recomeçar do zero, pode resgatar um sistema construído sobre conceitos falhos.

As abstrações também são importantes para os usuários. Usuários novatos querem programas cujas abstrações sejam simples e fáceis de entender; especialistas querem abstrações que sejam robustas e gerais o suficiente para serem combinadas de novas maneiras. Quando boas abstrações estão ausentes no design, ou se deterioram à medida que o sistema evolui, o programa resultante desenvolve uma crosta de complexidade. O usuário é então forçado a dominar uma massa de detalhes espúrios, desenvolver soluções alternativas e aceitar falhas frequentes e inexplicáveis.

O cerne do desenvolvimento de software, portanto, é o design de abstrações. Uma abstração não é um módulo, ou uma interface, classe ou método; é uma estrutura, pura e simples — uma ideia reduzida à sua forma essencial. (...) O processo de desenvolvimento de software deveria ser claro. Primeiro, você projeta as abstrações, a partir de uma consideração cuidadosa do problema a ser resolvido e suas prováveis variantes futuras. Então, você desenvolve suas incorporações no código: as interfaces e módulos, estruturas de dados e algoritmos (ou, na linguagem orientada a objetos, a hierarquia de classes, representações de tipos de dados e métodos).

Proposta:

- Adicionar no payload de resposta da URL do QR Code Dinâmico um campo opcional "pixAutomatico" cuja presença indica que existem dados sobre Pix Automático no payload. Esse campo seria um objeto que contém os dados relacionados ao Pix Automático. A ausência do campo "pixAutomatico" significaria que aquele pagamento não tem relação com o Pix Automático. Dessa forma, a adoção do Pix Automático poderia ser incremental, funcionando para todos os PSPs que se adaptarem sem quebrar a compatibilidade com os que ainda não houverem se adaptado ao Pix Automático.
- Adicionar o QR Code Dinâmico, inclusive com as funcionalidades de Pix Automático, como obrigatório a todos os PSPs recebedores, inclusive na interface móvel e web (app e internet banking).
- Utilizar o mesmo TxID para cobrança via QR Code Dinâmico ou cobrança via Pix Automático para impedir o pagamento duplicado da mesma obrigação. A importância desse tipo de medida já foi reconhecida em versões anteriores do MPI, ao dispor "A importância de que o txid seja enviado pelo usuário recebedor está relacionada à garantia da idempotência da API Pix. Dessa forma, evita-se a criação de múltiplas cobranças para uma mesma obrigação original, devido a uma falha na chamada da API que cause incerteza quanto a se a cobrança já teria sido criada ou não". A proposta aqui é que se mantenha esse objetivo como um valor inegociável no Pix e implementar essa garantia também no Pix Automático.
- Ao invés de criar uma entidade adicional CobR, deveria ser utilizado o mesmo recurso Cob ou CobV com um atributo idRec. O mesmo vale, aliás, para a CobV. Todos deveriam ser unificados para um único Cob, que fosse flexível, evoluível e adaptável o suficiente para que pudesse representar qualquer caso de uso de Pix.
- A ausência de uma interface móvel provida pelo PSP introduz um intermediário necessário (o ERP) em um arranjo que até então permitia, mas não obrigava o uso de intermediários. A ausência da obrigatoriedade de intermediários é fundamental para que a oferta de Pix Automático tenha um preço baixo, porque, mesmo que um intermediário decida cobrar mais do que o valor da comodidade ou funcionalidades próprias, o Pix Automático ainda assim estará disponível.

III.2. A especificação não deveria arquitetar jornadas específicas no código do Pix Automático

Premissa: o MPI sob consulta identifica e codifica de forma estrita e exhaustiva as jornadas possíveis para o Pix Automático. Evidências disso são, por exemplo: (i) a criação de entidades e estados exclusivos para a Jornada 1 (solicRec e estado rejeitado), (ii) a distinção

entre a Jornada 3 e a Jornada 4, que se dá na minúcia de haver duas telas ou uma tela de confirmação, (iii) o fato de o tipo de jornada adotada dever ser informada nas trocas de mensagens entre os PSPs, assim com se a operação ter sido iniciada via Open Finance, (iv) a proibição do uso do Pix saque/troco no contexto do Pix Automático, não por alguma preocupação específica com segurança, mas porque não se imagina hoje um uso possível da funcionalidade e não a sua inclusão demandaria trabalho de especificação e implementação adicional porque não estão sendo utilizadas abstrações que permitam o reuso de código (e especificação).

Análise: Relacionado ao tema do tópico acima, a especificação do MPI sob consulta faz o que chamamos de *arquitetura de experiências*. Isso quer dizer que a especificação sedimenta em código as experiências específicas que os usuários podem ter. São duas as consequências negativas disso: (i) há um trabalho adicional para replicar código de funcionalidades similares que poderiam ter sido simplificado por meio de uma abstração que incorpora o que há de comum em diversas funcionalidades para ser aplicado em diferentes situações, e (ii) qualquer evolução da experiência de usuários demandará uma nova mudança na especificação técnica e no código de cada um dos participantes do Pix para começar a ser testada. Para evitar esses problemas, a especificação técnica deveria construir blocos de funcionalidade que possam ser combinados de formas arbitrárias para construir experiências para o usuário final e não jornadas específicas. Da mesma forma, deveria definir primitivas que são reutilizadas na evolução do Pix e não prescrever de forma exaustiva tudo que pode acontecer no sistema.

Proposta:

- Substituir a solicRec pelo envio do link do QR Code Dinâmico (ou, caso não se entenda por unificar os dois links, o link URL de recorrência do QR Code Composto) para que a operação no PSP Pagador seja estritamente a mesma em qualquer caso de recebimento de solicitação de autorização de débito futuro — seja quando o usuário pagador escaneie um QR Code com Pix Automático, seja quando receba um pedido via ICOM. Além do link, a mensagem de envio da recorrência deveria conter o destino da mensagem (a ser preenchido com acesso à Chave Pix do usuário pagador) e o mesmo ID da autorização que estiver contido no *payload* de resposta da URL. Assim, a mensagem, com o seu endereçamento, conteria um ID de autorização que pode ser acessado na URL inserida na mensagem.
- Unificar os estados de solicitação de autorização de débitos futuros em todos os casos de uso. Confira-se no tópico III.4 a proposta de unificação.

III.3. A especificação deveria se valer da mecânica das Chaves Pix

Premissa: O Pix Automático não utiliza a mecânica das Chaves Pix. O endereçamento de contas dentro do Pix, contudo, deve ser feito utilizando as Chaves Pix tanto para a comodidade do usuário final quanto para facilmente permitir que um usuário final mude de PSP.

Análise: Em diversos pontos da proposta de manual do Pix Automático apresentada, as contas dos usuários finais, seja pagador ou recebedor, exigem o preenchimento de todos os dados de identificação das contas (banco, agência, conta e CPF/CNPJ e até mesmo ISBN do PSP). Embora a compatibilidade com outros arranjos seja importante para facilitar a adoção do Pix Automático (como no caso dos convênios utilities, por exemplo), é importante não prender o Pix Automático à forma antiga de endereçamento. O endereçamento no Pix é feito utilizando aliases (as Chaves Pix) exatamente porque o endereçamento direto (dados de conta) impedem que se modifique facilmente a origem ou o destino do pagamento. Essa facilidade de modificação unilateral pelo usuário final é o que permite a simplificação de procedimentos como a portabilidade, por exemplo.

Proposta: A nossa proposta é que se utilize, preferencialmente, as Chaves Pix para o endereçamento no Pix Automático e, para compatibilidade com autorizações já existentes, também se suporte o envio utilizando todos os dados, assim como foi feito no Pix iniciado pelo pagador com QR Code/Copia e Cola.

Essa proposta, no entanto, também exige uma mudança com respeito ao acesso à Dict. Uma vez que o Pix Automático passe a utilizar chaves, os PSPs participantes terão que fazer consultas adicionais à Dict nos seguintes momentos:

1. Quando o PSP recebedor enviar a SolicRec ao PSP pagador, terá antes que consultar os dados da Chave Pix do pagador.
2. Quando o PSP pagador for apresentar o pedido de autorização associado à SolicRec, deverá consultar a DICT para recuperar os dados do recebedor.
3. Quando o PSP recebedor enviar uma ordem de cobrança (CobR) ao PSP pagador, precisará consultar a DICT para receber o endereçamento atual do pagador.
4. Quando o PSP do pagador receber o pedido pagamento relacionado a cobrança (CobR), deverá consultar a DICT para encontrar o endereçamento atual do recebedor.

Todos esses acessos adicionais consumiriam tokens do mecanismo anti-scan da DICT. Para manter o mecanismo funcionando também deveriam ser atribuídos novos tokens ao PSP relevante quando essas mensagens passem pela ICOM. O PSP recebedor deverá receber um novo token por mensagem SolicRec e CobR enviada (casos 1 e 3) e o PSP pagador deverá receber novos tokens quando responder a SolicRec e quando confirmar o recebimento do pedido de pagamento (casos 2 e 4).

III.4. A especificação técnica deveria se valer das boas práticas de design de sistemas distribuídos, como facilitar idempotência.

Premissa: A proposta sugere que o ID de autorização, denominado idRec, seja um código sequencial que siga um padrão preditivo "RRxxxxxxxxxyyyMMddkkkkkkkkkk", prevê duas requisições (POST/locRec e post/rec) para criar cada pedido de autorização na API Pix e cria mais uma variante de Cobrança na especificação do Pix.

Análise:

- **ID de Autorização:** deveria ser um UUID para ser usado como chave de idempotência e remover a necessidade da requisição "POST /locrec" na criação de uma recorrência. A razão para a existência dessa requisição é a criação do id sequencial, que somente pode ser criado pelo controlador da sequência, o PSP recebedor. Uma vez removida essa restrição, o id (uuid) pode ser enviado na requisição "POST /Rec" sem nenhum prejuízo e esta requisição produz, na resposta, a location para o QR Code.

O envio de duas requisições para a criação de um único recurso (a Rec) reduz desnecessariamente a performance do uso de APIs e incentiva o uso de arquivos para troca de informações, que além de má prática de sistemas distribuídos, invariavelmente possuem uma latência substancialmente maior em seu processamento (processamento diário ou de hora em hora, por exemplo).

- Conforme exposto na proposta do item III.1. acima, porque existe uma distinção entre as diferentes formas de se cobrar pagamentos no Pix (Cob, CobV, CobR, potencialmente com TxIDs diferentes), se torna substancialmente mais difícil garantir o pagamento não seja feito em duplicidade, mesmo se valendo apenas do Pix. Hoje, no Pix, pode-se confiar que existirá apenas um ID para um mesmo pagamento, seja no passado ou futuro. Se a cobrança referente a uma mesma obrigação pode ir por duas formas diferentes e com ids diferentes, a plataforma Pix não é capaz de impedir a cobrança em duplicata e passa a depender que todos os ERPs, PSPs e demais participantes implementem a verificação de pagamento único e garantam que o pagamento em duplicidade não aconteça.

III.5. A especificação técnica deve permitir que o pagador sempre possa decidir como e quando o dinheiro sai de sua conta

Premissa: Em 7 pontos da proposta apresentada, encontramos situações onde o pagador não tem poder de decisão sobre como o dinheiro sai de sua conta:

1. A autorização é tudo ou nada: uma vez concedida a autorização, a única ferramenta à disposição do pagador é cancelar completamente a autorização. Essa medida drástica não

permite que o pagador se proteja de um aumento de cobrança indevido, como em um caso em que o recebedor é vítima de uma invasão de conta (Account TakeOver - ATO).

2. Caso a cobrança venha acima do valor máximo autorizado, a transação é negada automaticamente pelo PSP do pagador. Essa definição produz o efeito de incentivar o recebedor a aumentar o valor máximo, já que caso tenha algum aumento previsto não quer cancelar a autorização e criar uma nova. Para o pagador essa experiência também é ruim, porque aumenta o seu risco e, caso o pagamento acima do valor máximo tenha sido consentido, não será possível executá-lo.
3. O pagador possui janelas específicas dentro do dia do vencimento para efetuar o pagamento. Caso, por qualquer razão não possua liquidez em conta até a última janela, não terá como efetuar o pagamento, embora seja possível adicionar liquidez após a última janela de pagamento. Nesse caso terá que entrar em contato com o recebedor, para que esse gere uma nova ordem de pagamento (como um QRCode de cobrança) para conseguir efetuar o pagamento. Não existe um requisito técnico que exija que a experiência seja tão severamente degradada apenas porque o horário do pagamento
4. O pagador não tem como escolher qual pagamento é efetuado quando existem múltiplos pagamentos pendentes e não existe liquidez suficiente para pagar todos. Muitos brasileiros em diversos momentos precisam escolher quais contas pagar e quais não pagar. Essas escolhas geram juros e multas e nenhum PSP deve poder decidir quais serão pagas ou priorizadas nesse cenário.
5. O pagador tem a expectativa de poder efetuar pagamentos a qualquer momento, porque é assim que o Pix funciona até agora.
6. O pagador não possui um mecanismo para não participar do Pix Automático.
7. O pagador não consegue fazer portabilidade de seus pagamentos.

Análise: Com as seguintes 4 medidas simples e de fácil implementação pelos PSPs esses 7 problemas são sanados:

- As mudanças necessárias para evitar os problemas dos itens 1 e 2 são bastante simples. Basta modificar o conceito de “valor máximo para débito” para “valor máximo para débito sem autorização adicional” e passar o controle desse valor para o pagador. Com isso, o pagador pode optar por colocar o valor recomendado pelo recebedor ou um valor inferior. A cada cobrança recebida via Pix Automático, o PSP Pagador checa o limite e vê se é necessário uma autorização adicional. Nos cenários em que o pagamento seria negado por causa do valor máximo, agora o pagador pode tomar a decisão de pagar ou não. Isso também permite que o recebedor não precise colocar um valor máximo consideravelmente alto para cobrir possíveis variâncias de cobrança (como no caso de

pagamento de fatura de cartão de crédito, por exemplo) ou futuros aumentos, reduzindo o risco inerente da funcionalidade. O pagador também pode, agora, aceitar Pix Automático de empresas menos conhecidas, porque ele consegue definir o “valor máximo para débito sem autorização adicional” como zero reais, fazendo com que o PSP dele sempre entre em contato antes de autorizar o pagamento. Essas opções simples de serem adicionadas reduzem substancialmente o risco sistêmico do Pix Automático e facilitam a adoção da funcionalidade, porque agora o pagador se sente no controle sobre os pagamentos que executará.

- Os itens 3, 4 e 5, embora um pouco mais complexo que os anteriores, são corrigidos com uma pequena modificação: permitir que, a pedido do pagador, o pagamento possa ser liquidado imediatamente pelo canal primário. Entendemos que o objetivo de limitar o Pix Automático ao canal secundário de transações resulte do volume esperado de transações que, caso enviadas durante um pico diário de transações poderiam causar alguma degradação de performance. No caso de um pedido específico feito pelo pagador (apertar um botão na interface, por exemplo), esse risco não existe porque não será executado em massa e apenas simplifica um processo onde o pagador teria que entrar em contato com o recebedor para pedir a este que gere um QRCode para pagamento imediato. Essa funcionalidade também reduz o risco de acidentalmente ser gerado um pagamento em duplicata, porque o recebedor, por desatenção ou falta de funcionalidade em seu ERP, poderia gerar uma nova cobrança imediata e não cancelar a agendada.
- Para corrigir o item 6, uma funcionalidade de opt-out é fundamental. Embora entendemos que seja fundamental que o Pix Automático seja disponibilizado automaticamente para todas as contas, um mecanismo de opt-out total ou parcial também é fundamental. Além do pagador talvez simplesmente não ter interesse ou não querer correr o risco de uma possível fraude, também são possíveis abusos da funcionalidade para envio de mensagens indevidas. Um simples opt-out geral (o PSP Pagador automaticamente nega todos os pedidos de autorização) e um opt-out de uma origem (o PSP Pagador automaticamente nega todos os pedidos de autorização de um recebedor).
- O item 7 é um pouco diferente. É bastante razoável que o lançamento do Pix Automático não inclua portabilidade, reduzindo o tempo de desenvolvimento para o lançamento inicial. Mas para isso ser efetivo, a portabilidade já deve estar prevista e a infraestrutura proposta não deve impedir que a portabilidade seja implementada de maneira simples. A proposta atual permite que a portabilidade seja implementada através de um protocolo que envolva 3 PSPs: o PSP do recebedor, o PSP original do pagador e o PSP final do pagador. Mas uma outra pequena mudança bastante simples na especificação permite que essa portabilidade seja executada envolvendo apenas o PSP original e final do pagador. Basta que se utilize a chave Pix do pagador na autorização e envios de cobrança. Com

isso, o PSP do recebedor passa a sempre buscar na Dict para qual banco e conta deve enviar a cobrança e a simples portabilidade da chave poderia incluir a portabilidade do pagamento. Isso também reduziria a fricção que o pagador tem para aderir ao Pix Automático, porque passaria a ter que passar apenas a chave Pix ao invés dos dados de banco, agência, conta e CPF/CNPJ.

A portabilidade parcial também é possível, mas com um custo um pouco maior. Seria necessário permitir a alteração do campo chave Pix da autorização de débitos (SolicRec) pelo usuário pagador e essa informação deveria ser propagada ao PSP do recebedor. É possível reutilizar a resposta da SolicRec mudando um pouco a sua semântica (podendo ser enviada múltiplas vezes), mas é uma mudança um pouco maior que as mencionadas até o momento.

Essas 4 medidas bastante baratas em termos de custo de implementação e especificação (i) reduzem substancialmente o risco sistêmico de segurança por reduzir os limites de pagamento automático e (ii) aumentam consideravelmente o alcance, casos de uso e controle que o pagador possui sobre como seus pagamentos são executados. Ambas contribuem fundamentalmente para a adoção do Pix Automático.

III.6. Campos do payload JSON dos parâmetros de recorrência no QR Code Composto e entidades do Pix Automático:

Premissa: O campo 1.1 do payload JSON é o do identificador da recorrência, denominado idRec e de tipo String. Esse campo corresponde ao atributo idRec da entidade Rec no contexto do Pix Automático. No detalhamento sobre o atributo idRec da entidade Rec, a proposta especifica o formato que o idRec deve assumir:

“RRxxxxxxxxxyyyyMMddkkkkkkkkkkk”, com 29 caracteres “case sensitive”, sendo: R ou C – fixo (1 caractere). “R” caso a recorrência tenha sido criada dentro do Pix, ou “C” caso tenha sido criada pela trilha do Open Finance; R ou N – fixo (1 caractere). “R” caso a recorrência permita retentativas de realização do débito em data posterior à data de agendamento original, ou “N” caso não permita retentativas. xxxxxxxx – identificação do agente que presta serviço para o usuário recebedor que gerou o <Id>, podendo ser: o ISPB do participante direto, o ISPB do participante indireto ou os 8 primeiros dígitos do CNPJ do prestador de serviço de iniciação (8 caracteres numéricos [0-9]); yyyyMMdd – data (8 caracteres) de criação da recorrência; kkkkkkkkkkkk – sequencial criado pelo agente que gerou o <Id> (11 caracteres alfanuméricos [a-z|A-Z|0-9]). Deve ser único dentro de cada “yyyyMMdd”.

Análise: O idRec deve ser um UUID com 128 bits de entropia. Tal como proposto, o ID possui 65 bits ($\log_2(62^{11})$) de entropia para uma recorrência criada em um dia por um PSP. Se houver uma URL exposta pra internet que resolva esse id para os dados associados a ele, 65 bits de entropia não é considerado seguro. Além disso, o ID de uma recorrência não

deveria conter informação sobre se permite ou não retentativas. Qualquer metadado associado a isso deveria estar no payload de recorrência e não no ID. Caso se entenda que o ID deveria conter informações específicas (o que recomendamos evitar), não há por que fazer a distinção na especificação entre jornada iniciada via Open Finance ou via Pix. Da mesma forma, o elemento “xxxxxxx” do ID não deveria existir. Não há por que identificar qual PSP gerou o ID. A identidade do PSP que enviou o pedido de autorização estará bem definido na troca de mensagens via SPI e pelo domínio da URL do QR Code Dinâmico (ou do QR Code Composto). O importante é que o ID está associado a um usuário recebedor. Até porque, no caso de o usuário recebedor no futuro fazer a portabilidade para um outro PSP, a existência de referência ao PSP antigo no ID da recorrência pode gerar inconsistências e erros.

Premissa: O campo 2.3 do payload JSON é o do identificador do contrato, denominado `vinculo.contrato`. Na descrição dos campos do payload JSON, o identificador do contrato é especificado como uma string, mas no mapeamento da `pain.009`, o atributo `vinculo.contrato` é definido como um número.

Análise: No mapeamento da `pain.009`, o identificador de contrato deve ser uma string sem limitação sobre caracteres (número ou letras). Esse identificador é externo ao sistema, bastando que os PSPs repassem a informação. Assim, não há por que estabelecer um formato (número) e obrigar que recebedores transformem seus identificadores de contrato em números.

Premissa: O campo 3.3 do payload JSON é o da periodicidade, denominado `calendario.periodicidade`, de tipo String. Na [documentação da API Pix](#), o campo é definido como podendo receber os valores: "SEMANAL", "MENSAL", "TRIMESTRAL", "SEMESTRAL" ou "ANUAL".

Análise: Não deveria precisar ser uma periodicidade fixa. É restrição desnecessária dado que o PSP Recebedor envia o pedido de pagamento cada vez via SPI. Da forma como proposto, não está claro como o PSP Pagador deve fazer a verificação entre autorização e cobrança do Pix Automático com relação à periodicidade. Hipótese: se for semanal e o vencimento cair em uma sexta-feira feriado local e o PSP Recebedor só enviar a cobrança na segunda-feira seguinte. Como o PSP Pagador deve fazer a verificação de periodicidade? A primeira semana não terá cobrança e a seguinte terá duas cobranças. Como o PSP Pagador fará a distinção entre esse caso e o caso de o PSP Recebedor enviar por erro ou malícia uma cobrança adicional em uma semana qualquer? Nossa sugestão é que a periodicidade seja uma string livre, inclusive para ser devolvida sem valor para autorizar uma única transação futura, e que o PSP Pagador não seja obrigado a fazer esse tipo de verificação. No cenário em que nossas propostas são incorporadas, caso o recebedor tivesse que enviar duas cobranças na mesma semana devido a feriados, o pior que poderia acontecer é que, ao invés de cancelada, a

segunda cobrança exigiria a autorização adicional do pagador, reduzindo para ambos o trabalho para o cumprimento da obrigação.

Premissa: O campo 5.1 do payload JSON é o do CPNJ do usuário recebedor, denominado `recebedor.cnpj` e de tipo String. Já o atributo recebedor da entidade Rec é definido como "a identificação do usuário recebedor. Ele não será informado pelo próprio usuário no momento de criação da recorrência. O PSP Recebedor deverá preenchê-lo de acordo com os dados cadastrais do usuário que está se conectando com ele via API Pix". Por fim, o atributo `contaRecebedor` da entidade cobR é definido como contendo "informações bancárias, que deverão ser informadas em todas as cobranças". Nesse ponto, o manual posto em consulta também define que o "PSP Recebedor deverá validar se o recebedor é o titular da conta informada", bloqueando cobranças em caso negativo

Análise: O dado de CNPJ do usuário recebedor deveria ser obtido por meio de consulta à Chave Pix do usuário recebedor, conforme já mencionado. A inclusão da Chave Pix tanto na entidade Rec quanto na entidade cobR acrescentaria uma camada de verificação para o PSP Pagador sem dificultar a portabilidade de PSP Recebedor. Caso fosse utilizada a Chave Pix no atributo `contaRecebedor` da entidade cobR, o PSP Recebedor poderia confiar na validação da DICT sobre a titularidade da chave, dispensando a validação no momento da transação e acelerando essa operação.

Premissa: O campo 5.3 do payload JSON é o do ISPB do usuário recebedor, denominado `recebedor.ispbParticipante` e de tipo String.

Análise: Pelas razões expostas acima, deveria ser a Chave Pix do usuário recebedor.

Premissa: A proposta cria um atributo `politicaRetentativa` na entidade Rec que "guarda a informação sobre a habilitação ou não de retentativas após o vencimento", sendo que as opções, segundo a especificação, seriam não permitir ou permitir até 3 retentativas no prazo de 7 dias corridos.

Análise: Como já mencionado, o usuário pagador precisa ter a escolha sobre aceitar a cobrança com juros ou multa automática ou não. Melhor que um atributo *política retentativa* seria utilizar o atributo já existente no payload do QR Code Dinâmico com vencimento (que, a propósito, também deveria ser um só independentemente da existência de data de vencimento): **calendario.validadeAposVencimento**. Este é o atributo que, no arranjo Pix, deveria significar a possibilidade de cobrança mesmo em caso de uma cobrança ativa não ter sido paga até o seu vencimento. Além disso, a Cob (ou, caso seja mantida a COBR como uma entidade à parte, a CobR) deveria ter um estado adicional: *atrasada*, que não é comunicada entre PSPs, mas atualizada em cada PSP, para o caso de o usuário pagador não ter pago e o

usuário recebedor aceitar manter a cobrança ativa e atualizada para pagamento posterior caso o usuário pagador queira.

Premissa: A proposta cria um atributo encerramento na entidade Rec, que “contém informações sobre a rejeição ou o cancelamento de uma recorrência”.

Análise: Como já mencionado, a distinção entre cancelamento e rejeição apenas agrega complexidade ao sistema e deveria ser unificada.

Premissa: A proposta cria um atributo ativação na entidade Rec, que traz "informações sobre a jornada de autorização que foi utilizada para a confirmação da recorrência". Nesse ponto, a proposta detalha que o campo tipoJornada seria preenchido pelo PSP Pagador “de acordo com o código da mensagem de confirmação da autorização (PAIN.012), que identificará se foi Jornada 1, Jornada 2, Jornada 3 ou Jornada 4”.

Análise: O PSP Pagador não deve ser obrigado a informar qual jornada/experiência foi utilizada para efetuar o pagamento/autorizar recorrência. Dados sobre isso podem ser obtidos por meio da criação de um relatório obrigatório aos PSPs. Não se justifica o engessamento da experiência do usuário ao incluir esse dado na especificação técnica e no código de cada um dos participantes.

Premissa: A entidade SolicRec foi criada exclusivamente para a Jornada 1 e corresponde à solicitação de confirmação de recorrência.

Análise: A solicitação de confirmação de recorrência é específica para a Jornada 1 de autorização do Pix Automático. Deveria se limitar ao link URL do QR Code Dinâmico, que deveria ter campos opcionais para o Pix Automático. Caso não se entenda por unificar os canais de comunicação direta entre PSP Pagador e PSP Recebedor, a SolicRec deveria se limitar a enviar o link URL da recorrência. Em último caso, a solicRec deveria ao menos incluir exclusivamente o mesmo payload devolvido pelo link URL da recorrência, além dos dados de endereçamento da mensagem, que deve ser retornado pela consulta à Chave Pix do usuário pagador. Isso porque ter mensagens diferentes para cada forma de solicitação de autorização de Pix Automático aumenta muito a complexidade do sistema.

SolicRec e Rec representam o mesmo recurso, então deveriam ser representadas da mesma forma. A distinção entre Rec e SolicRec não facilita a construção do Pix Automático, apenas aumenta a dificuldade de se implementar a API de forma idempotente. A única distinção relevante entre as duas mensagens seria sobre um estado específico, mas que de qualquer forma deveria existir apenas entre recebedor e PSP recebedor, não sendo propagados ao PSP pagador. O PSP pagador deve apenas ser capaz de observar os seguintes estados: enviada, recebida, aceita, atrasada, cancelada e expirada. O estado "criada" deve existir apenas entre

recebedor e seu PSP. O estado "atrasada" deveria ser incluído, conforme exposto no comentário ao item 2.1.5 acima.

Premissa: No diagrama de estados do COBR da página 91, se lê na imagem "COBR - paga na data normal".

Análise: Pagamento "na data normal" deveria ser trocado para "antes de vencido", porque enquanto a cobrança está "ativa" o pagador deve ter a opção de antecipar o pagamento.

III.7. Sobre o cancelamento de agendamento de pagamento de cobrança recorrente e o cancelamento de recorrência

Premissa: A solicitação de cancelamento de agendamento de pagamento de cobrança recorrente pelo usuário recebedor deve ser recebida pelo PSP Pagador até as 22h00 do dia anterior à data prevista para o pagamento. A solicitação de cancelamento de uma recorrência pelo usuário recebedor não está condicionada a janelas de horário. Quanto ao usuário pagador, esse somente pode cancelar o pagamento "antes da data de liquidação original", mas não pode "cancelar o agendamento de uma retentativa após o vencimento".

Análise: O cancelamento do agendamento da cobrança recorrente continua condicionado à janela de horário, o que implica que o Pix Automático apenas acontece na janela secundária. O cancelamento da recorrência, contudo, não é condicionado à janela de cancelamento do agendamento da cobrança. O cancelamento da recorrência deve cancelar os agendamentos de cobrança associados. Logo, cancelar a recorrência pode cancelar os agendamentos de cobrança fora da janela de cancelamento. Dada a importância de os usuários pagador e recebedor terem controle sobre o seu dinheiro e suas cobranças, não deveria haver janelas para o cancelamento de cobranças em um arranjo de pagamentos instantâneos.

III.8. Comentários adicionais pontuais

- Sugerimos denominar o item 2.8.4.2 de recPayload, que é mais tarde referenciado no Atributo SolicRec, mas que não foi definido ou denominado dessa forma antes na versão do MPI posto em consulta.
- A nomenclatura empregada no manual posto em consulta, embora talvez normalmente utilizada no setor financeiro, se distancia da nomenclatura utilizada na regulação do arranjo, dificultando o entendimento e facilitando que erros ocorram por desatenção. Recomendamos que ao invés de Rec e recorrência, seja utilizada a palavra Autorização, que já figura na regulação do arranjo, para que seja claro ao que entidades como Rec e SolicRec se referem. Também recomendamos que seja utilizado o termo Instrução de Pagamento ao invés de CobR ou cobrança recorrente.