TAP2PIX.org

Um padrão de pagamento por aproximação aberto para todos

Análise Técnica

Proposta enviada pelo BC para utilização do Pix por aproximação

Análise do fluxo proposto pelo BC

TAP2PIX.org

Sexta-feira passada (23/08/2024) o BC abriu para o GT a proposta de padronização do Pix por Aproximação

O Banco Central do Brasil, por meio do Grupo de Trabalho de Padronização e Requisitos Técnicos, iniciou uma consulta sobre a proposta de padronização para pagamentos com PIX por Aproximação + Iniciador de Pagamentos no contexto do Open Finance, utilizando a Jornada Sem Redirecionamento (JSR).

Segundo em redes sociais, o fluxo consiste no envio por meio do APDU de uma URI padronizada pelas Maquininhas, Smartphones ou Pin Pads

URI do PIX

O formato esperado de URI para utilização do TapNPix segue o padrão:

```
pix://<hostname>?qr=<uri-encoded-emv-qr-string>&sig=<signature>
```

TAP2PIX.org

Conclusão sobre a proposta enviada

O projeto Tap2Pix concorda plenamente com o que foi proposto pelo BC!

O Banco Central brilhantemente identificou uma solução inovadora que contempla dois métodos, os quais podem ser executados de três maneiras distintas.

O primeiro método utiliza o recurso de APDU, criando um canal direto de transmissão. Através desse canal, é possível enviar dados mais sensíveis com menor criptografia (Como por exemplo apenas dados no padrão EMV de cartões smart). Contudo, é necessário que o cliente abra o aplicativo ou wallet e selecione a opção de leitura do NFC, para que o processo de leitura seja iniciado. Mesmo que a Apple abra os recursos de NFC (Analisaremos o comunicado nas próximas páginas), ainda sim precisará que o APP seja aberto e acionado a leitura do NFC dentro do mesmo.

O segundo método envolve o uso de Deep Links. Esses links apresentam vulnerabilidades, pois não possuem uma entidade específica, permitindo que qualquer aplicativo possa reivindicar sua autoria. No Android, o Deep Link solicita ao usuário que escolha qual aplicativo deve ser aberto, enquanto no iOS, o último aplicativo se apropria dessa invocação. Contudo, no contexto do Deep Link proposto, também há o envio de um parâmetro de signature (assinatura). Isso garante que os dados contidos no campo URI Encoded EMV QR String possam incluir qualquer informação, uma vez que são criptografados com a assinatura que segue o padrão criptográfico PS256.

O terceiro método, considerado pelo projeto Tap2Pix utiliza o Universal Link + Copie e Cole. Acreditamos que esse formato, seja uma solução eficaz para contornar limitações atuais. **O Universal Link substituiria o Deep Link**, e por serem geridos por uma entidade com um domínio próprio e possuírem certificado RSA, possibilita o aumento da segurança e a invocação do **Super Wallet Instantâneo** e multiplataforma. Essa abordagem melhora significativamente a usabilidade da transmissão via NFC, permitindo que apenas aplicativos com domínio registrado na Apple Store e Google Play possam ser executados de forma imediata. Além de facilitar a usabilidade, o wallet instantâneo promove a democratização do uso do NFC e apoia toda a jornada gradual de adaptação dos clientes com as tecnologias como: links, QR codes e NFC, além de trabalhar nas jornadas com redirecionamento e sem redirecionamento. Vale ressaltar também que esse formato é o único exequível em curto e médio prazo. Muito antes do lançamento do JSR, além de ser o único a trabalhar a **Jornada COM Redirecionamento.**

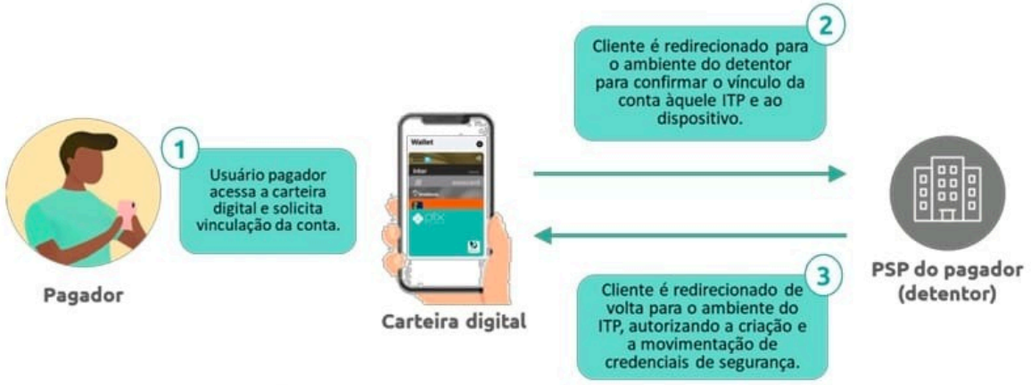
TAP2PIX.org

O que seria APDU?

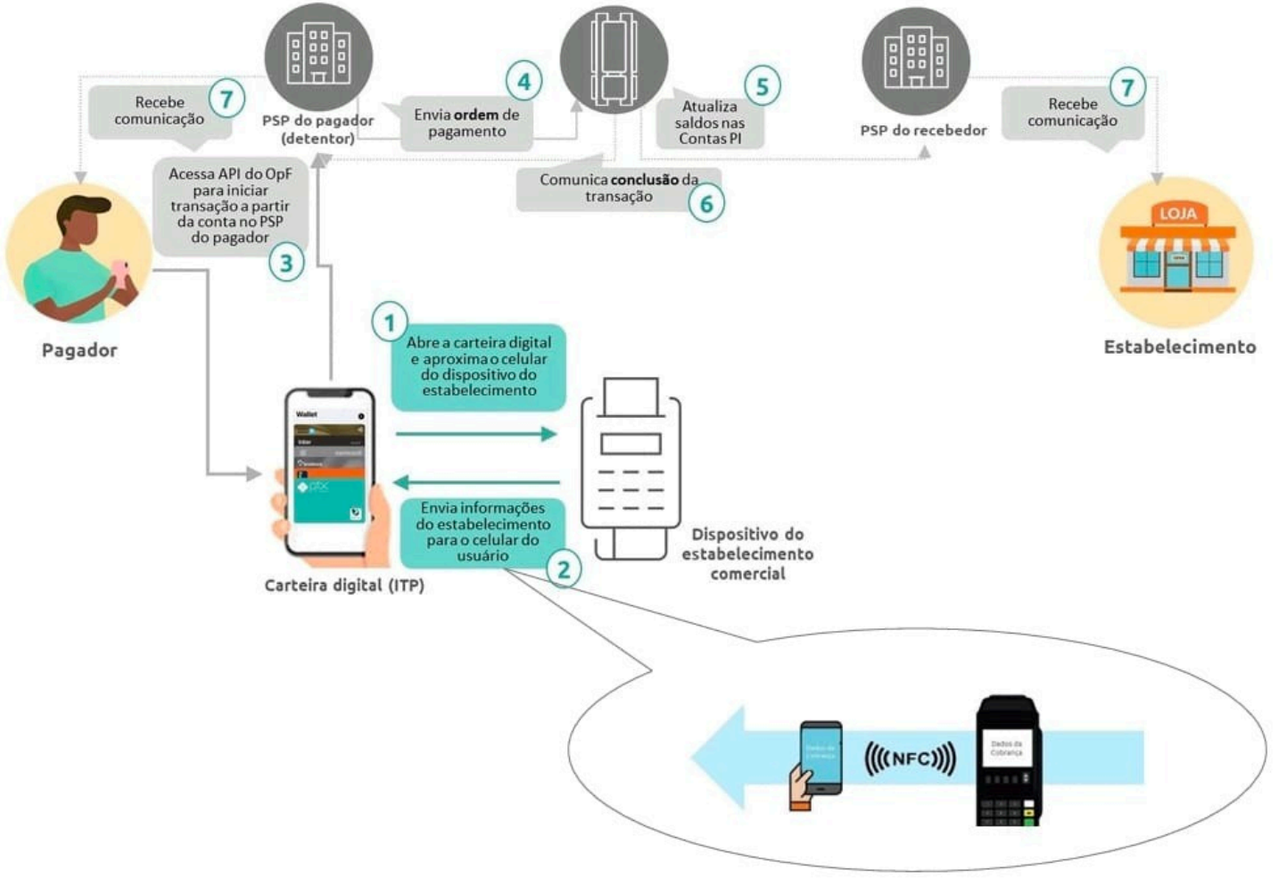
APDU significa "**Application Protocol Data Unit**" e é um conjunto de comandos usados para enviar informações de um dispositivo para outro. É usado principalmente na comunicação entre um cartão inteligente (como um cartão de crédito) e um terminal de pagamento. O APDU contém instruções específicas que o cartão inteligente deve executar e os dados que devem ser transmitidos. Em resumo, o APDU é um padrão de comunicação que permite que dispositivos se comuniquem de forma eficiente e segura. **Esse método é o único aplicável a cartões EMV ou Smart Cards.**

É importante ressaltar que, apesar da recomendação de uso do APDU, o sistema de pagamentos Pix já conta com uma robusta estrutura de criptografia de curva elíptica, uma forma avançada de criptografia assimétrica, e módulos de segurança de hardware (HSM) para proteger a comunicação entre os sistemas.

Portanto, o uso do APDU está inserido de forma redundante em um amplo conjunto de medidas de segurança já existente no Pix. Além disso, a estrutura proposta pelo BC inclui um campo OPCIONAL de assinatura, com o algoritmo PS256, reforçando ainda mais a segurança do sistema com uso de Deep Link. A proposta da Tap2Pix foca no uso do Universal Link, onde possui uma entidade e certificado RSA. O que garante uma segurança elevadíssima somado com o incrível legado de uso do copie e cole nos e-commerces de todo o Brasil mesmo usando os navegadores.



2.3.2. Fluxo da transação



Material em desenvolvimento / Sujeito a alterações

Diagrama de sequência (caso Android)

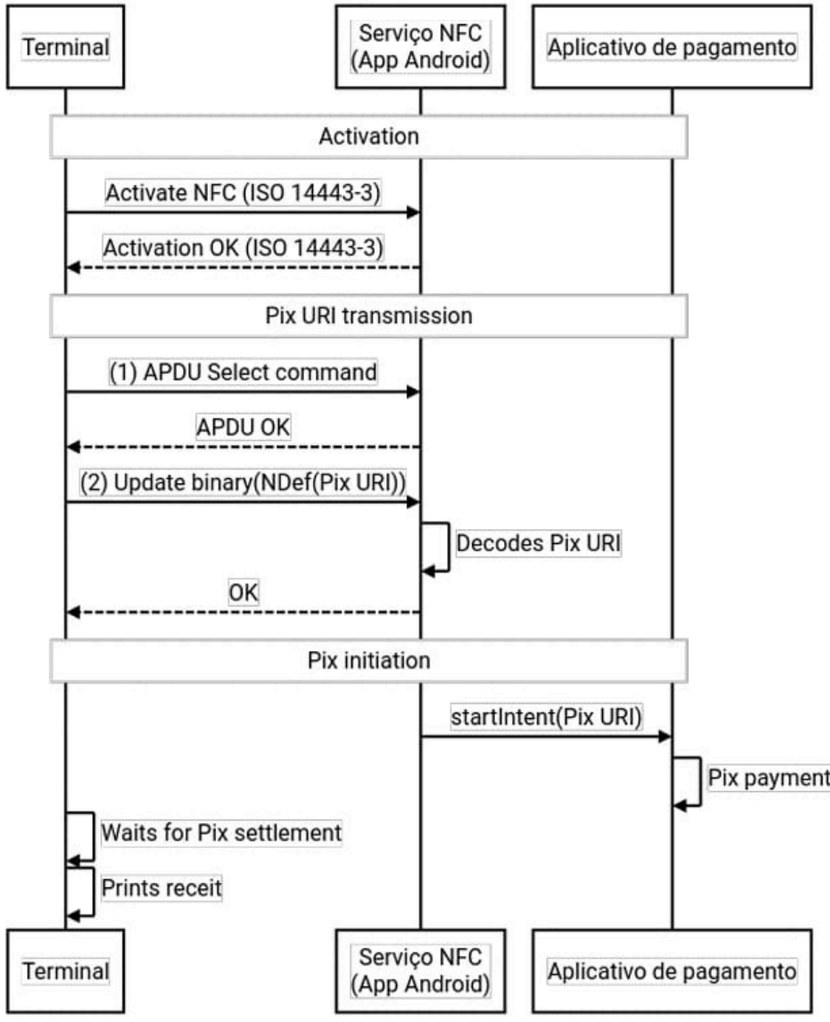


Diagrama 1: Sequência de mensagens trocadas entre Terminal, Serviço NFC do Android e Aplicativo de pagamento

Material em desenvolvimento / Sujeito a alterações

Protocolo

O protocolo de captura de QR codes via NFC, denominado “Tap to Pix”, compreende:

1. Na definição de URI a ser resolvida para iniciação de pagamento PIX;
2. No diagrama de sequência para a captura via NFC.

Premissas

O terminal deve possuir capacidade de transmitir conteúdo via NFC para o sistema operacional do dispositivo utilizando o padrão NDEF para transmissão de URIs através de comandos APDU, em acordo com a documentação do sistema operacional. No sistema operacional Android, a estrutura é NDefRecord.
A captura não está restrita a terminais POS, podendo se estender para outros dispositivos compatíveis com NFC como celulares ou pin pads.
Este protocolo é aberto, isto é, o TapNPix pode ser utilizado por quaisquer aplicativos compatíveis com o sistema operacional do dispositivo do pagador.

URI do PIX

O formato esperado de URI para utilização do TapNPix segue o padrão:

```
pix://<hostname>?qr=<uri-encoded-emv-qr-string>&sig=<signature>
```

Os placeholders devem ser substituídos de acordo:

- <hostname>: identificação do domínio que gerou o QR code;
- <uri-encoded-emv-qr-string>: conteúdo do PIX copia-e-cola codificado em URI. Veja a referência encodeURIComponent().

Parâmetro reservado para uso futuro:

- <signature>: parâmetro opcional com a assinatura do código “Copia e Cola” decodificado. A assinatura deve seguir o algoritmo PS256, conforme padrão atualmente praticado no Open Finance Brasil. A disponibilização da chave pública para a parte recebedora para fins de validação segue sob definição.

O tamanho máximo da URI é estimado em cerca de 422 bytes, desconsiderando o tamanho do domínio e o overhead da codificação Percent-Encoding.

Este formato permite que parâmetros adicionais sejam negociados e incorporados à especificação conforme a evolução do produto.

TAP2PIX.org

Sendo assim, podemos concluir que o movimento de iniciação de um pagamento com Pix utilizando o NFC, fará um fluxo diferente do que temos hoje com os Cartões de Credito junto as wallets.

Isso ocorre, porque a conclusão do pagamento ocorrerá no celular do cliente e não junto ao vendedor.

É importante notar que todo o fluxo proposto até o presente momento não funciona no IOS com a Apple Wallet e por isso no material foi citado o fluxo utilizando o sistema operacional Android como base.

Vale ressaltar que a utilização junto ao Apple Pay, somente funciona com padrão EMV e sem processamento de APIs pelo lado do pagador.

Sendo assim, vamos abstrair o estudo de uso com Apple Pay e focar no Wallet Apple que a própria Apple publicou documentos onde informa que abrirá o seu uso, como visto a seguir

TAP2PIX.org

Colocando os Pingos nos Is

O mercado tem se equivocado bastante sobre as diferenças entre as tecnologias, os fluxos, gratuidades,… pois bem vamos destrinchar essas informações:

Primeiramente, o que foi liberado junto a UE (União Europeia) é diferente do que será liberado ao Brasil. Isso porque a UE se beneficia de um acordo feito com a Apple que permitirá a gratuidade por 10 anos de uso do NFC.

A Apple também já informou que irá liberar no **IOS 18.1 (somente Iphones acima do 11)** para a Austrália, **Brasil**, Canadá, Japão, Nova Zelândia, Reino Unido e Estados Unidos o acesso ao NFC utilizando o **SE (Elemento Seguro)** e que haverá **royalty fee por transação** junto as empresas desenvolvedoras.

LEITURA RÁPIDA • 14 de agosto de 2024

Desenvolvedores poderão oferecer transações por NFC usando o Elemento Seguro em breve

Veja mais em: https://www.apple.com/br/newsroom/2024/08/developers-can-soon-offer-in-app-nfc-transactions-using-the-secure-element/

TAP2PIX.org

Colocando os Pingos nos Is

Ela coloca também que:

"Os usuários podem **abrir o app diretamente** ou **defini-lo como o app padrão** para esse tipo de transação nos Ajustes do iOS **e apertar duas vezes o botão lateral** do iPhone para iniciar uma transação."

"Para incorporarem essa nova solução nos apps para iPhone, **os desenvolvedores precisarão aceitar um acordo comercial com a Apple, solicitar os direitos para usar o NFC e o Elemento Seguro e pagar as taxas associadas. Isso garante que apenas os desenvolvedores autorizados que atendem a determinados requisitos regulamentares** e do setor e se comprometem com os padrões contínuos de segurança e privacidade da Apple possam usar as APIs relevantes. “

LEITURA RÁPIDA • 14 de agosto de 2024

Desenvolvedores poderão oferecer transações por NFC usando o Elemento Seguro em breve

Veja mais em: https://www.apple.com/br/newsroom/2024/08/developers-can-soon-offer-in-app-nfc-transactions-using-the-secure-element/

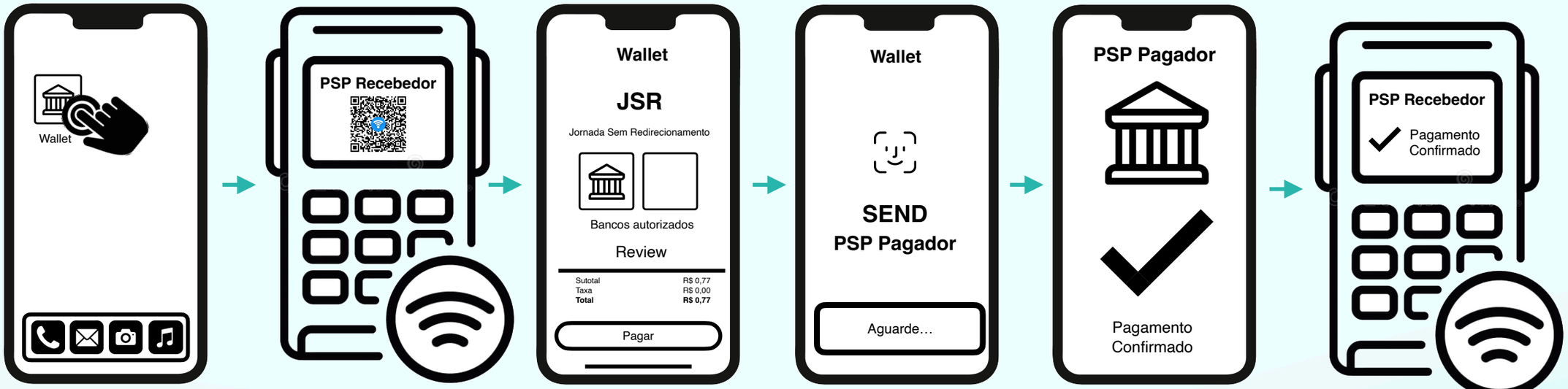
TAP2PIX.org

Destacando os pontos importantes:

1. **Gratuidade somente na UE:** Somente a União Europeia (UE) oferece a gratuidade de uso do NFC por 10 anos.
2. **Acesso à Internet:** Será necessário que tanto o vendedor quanto o pagador tenham acesso à internet.
3. **Compatibilidade com iPhone:** As funcionalidades de leitura do NFC estarão disponíveis no iPhone a partir do iOS 18.1, excluindo todos os iPhones inferiores ao modelo 8 e os que não estão atualizados para a versão do iOS 18.1.
4. **Abrir app para ler o NFC:** A atualização para o iOS 18.1 permitirá a leitura do NFC somente após o aplicativo ser aberto.
5. **Personalização do clique duplo lateral:** O iOS 18.1 permitirá a configuração para abrir o app ao apertar duas vezes o botão lateral.
6. **Taxas e Acordo Comercial com a Apple:** Desenvolvedores precisarão aceitar um acordo comercial com a Apple e pagar taxas para utilizar o NFC e o Elemento Seguro.
7. **Transação do Lado do Cliente:** A transação ocorrerá do lado do cliente/pagador, e não do vendedor.
8. **Envio de URI via APDU:** Uma string de URI será enviada via APDU, permitindo a cópia e colagem.
9. **Funções do APDU:** O APDU da Apple Wallet hoje não possui a função de processamento de pagamento e leitura do NDefRecord.
10. **Leitura APDU e NDef:** Na atualização 18.1, a Apple permitirá que apps leiam APDU e NDef após estarem abertos, exigindo que o cliente abra o app (com 2 cliques no botão lateral) e clique em ler o NFC.
11. **Execução Automática do NFC:** O NFC não será executado automaticamente ao aproximar o celular.
12. **Adesão dos Bancos ao JSR:** Não será necessária a adesão dos bancos ao JSR para executar pagamentos via NFC, já que a conta do cliente já estará ativa no app.
13. **Função do JSR:** O JSR faz sentido somente para wallets ou apps bancários que atuem como HUB integrador para pagamentos com contas de outros bancos.
14. **Latência e Erros no JSR:** O JSR poderá apresentar latência (demora no processamento) e erros na devolução do Request de processamento do lado do PSP do pagador e recebedor, devido ao uso de múltiplas conexões entre o banco e os PSPs.
15. **Exclusão de Não Participantes:** Não participantes obrigatórios do JSR e BaaS estão excluídos do pagamento via NFC e do Open Finance.
16. **Apenas Autorizados:** Conquistar junto a Apple a autorização de uso do NFC continuará sendo uma tarefa extremamente burocrática. Há inclusive relatos junto a UE que a Apple esta fazendo um controle rigoroso, dificultando assim a utilização do NFC junto as fintechs.
17. **Adesão ao JSR pelas adquirentes:** As adquirentes precisarão aderir ao Open Finance e conquistar a autorização de ITP para inclusão do JSR em seu sistema.
18. **UX e aceitação cultural:** O JSR será uma atualização incrível, mas precisa ser motivado a sua adesão de forma gradual a ponto do cliente se sentir seguro em dar autorização de saque direto em seu PSP.

TAP2PIX.org

Fluxo para pagamento por aproximação com JSR



TAP2PIX.org

Fluxo para pagamento por aproximação com JSR

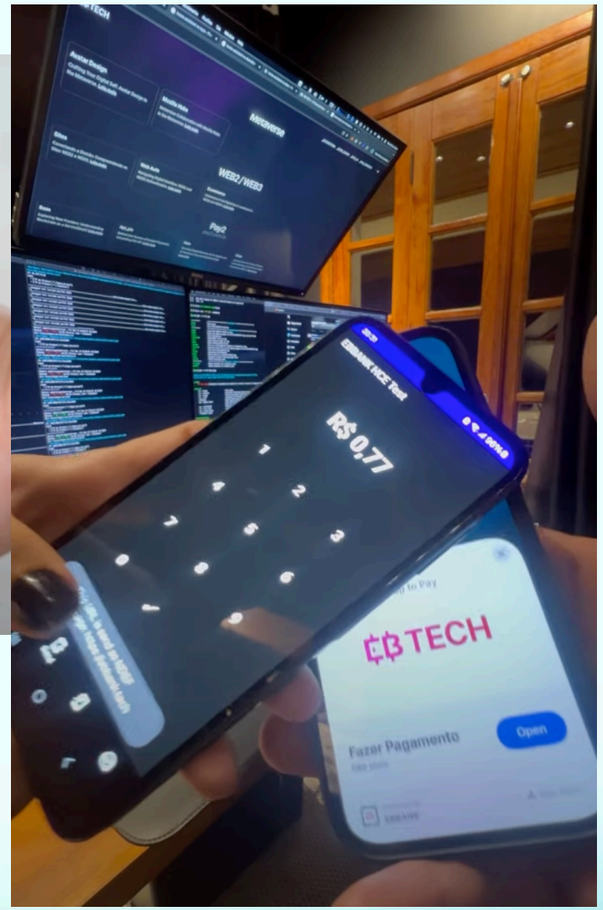
1. O Cliente abre o app Wallet e aproxima do POS;
2. O POS inicia o pagamento ao gerar um QR Code;
3. O POS envia o QR Code no padrão URI pix://<hostname>?qr=<uri-encoded-emv-qr-string>&sig=<signature> e o entrega via NFC com o APDU;
4. O cliente abre o app e aproxima o dispositivo móvel de um terminal POS;
5. O dispositivo do cliente recebe o APDU com a URI pix://<hostname>?qr=<uri-encoded-emv-qr-string>&sig=<signature>;
6. Cliente seleciona a conta (pré-autorizada ou banco) e inicia a transação através do Open Finance, utilizando a Jornada Sem Redirecionamento;
7. Autenticação biométrica no dispositivo do cliente confirma a transação para o PSP do pagador.
8. PSP do pagador valida e debita o valor da conta do cliente;
9. Crédito é transferido do PSP do pagador para o PSP do recebedor (merchant), finalizando a transação;

APP

TAP2PIX.org

Como funciona o projeto Tap2Pix?

[Link do video apresentação do Tap com Alipay]



[Link do video do POC]

TAP2PIX.org

Benefícios de uso do Universal Link + QR Code

Como proposto pelo projeto de padronização Tap2Pix

Benefícios do uso da padronização do Tap2Pix na jornada COM redirecionamento e jornada SEM redirecionamento:

- Adaptação da usabilidade com os clientes utilizando o NFC: Em caso de defeito do leitor de NFC, que é comum em celulares que tiveram a parte traseira trocada ou em modelos mais antigos que não possuem NFC, o cliente ainda terá a opção de leitura do QR Code. Isso também promove uma adesão gradual e entendimento da usabilidade de uso do NFC.

- Gradual adaptação das Instituições Financeiras (IFs), Instituições de Pagamento (IPs) e adquirentes junto ao Open Finance: Ao utilizar o universal link com o "copie e cole", todos os bancos não obrigados continuarão a realizar pagamentos normalmente, mantendo o mesmo fluxo.

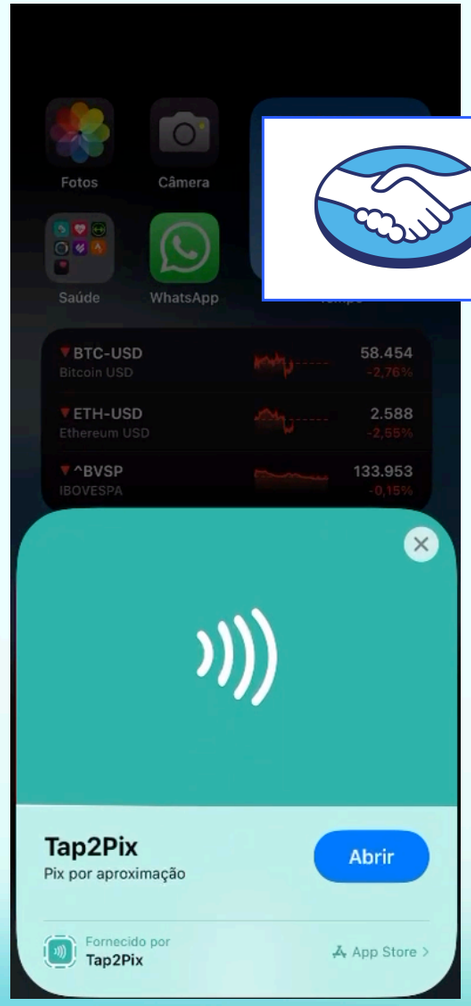
- Legado e Segurança Ratificada: Todos os e-commerces utilizam o “copie e cole” nos navegadores ao salvar no clipboard/memória antes de acessar o aplicativo do banco. A grande maioria dos apps bancários já ficam escutando o clipboard do device, onde detectam CPF, E-mail, Celular e o copie e cole, onde sugerem transferência ou pagamento.

Assim, a proposta do **tap2pix.org** foca na democratização e na adaptação gradual do mercado (clientes e instituições). Criando uma Wallet multiplataforma, aberta e com uma usabilidade incrivelmente simples.

A utilização de aplicativos instantâneos possibilita o uso imediato da Wallet, sem a necessidade de autorização ou cadastro prévio. Isso a torna uma solução versátil tanto para o JSR (Jornada sem Redirecionamento) quanto para o JCR (Jornada com Redirecionamento).

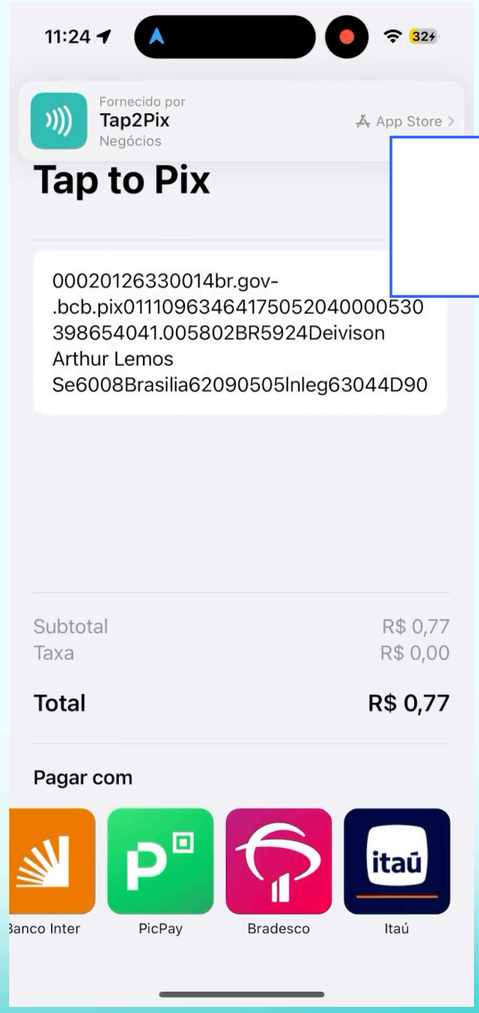
TAP2PIX.org
Wallet

Demonstração com Mercado Pago e Itau



mercado pago

Link do vídeo



Itaú

Link do vídeo

Benefícios de uso do padrão Tap2Pix

- Usabilidade familiar e amplamente conhecida com o “Copie e Cole”.
- Segurança reforçada com o app bancário de seu uso cotidiano;
- Respeito à privacidade e à LGPD.
- Sem pagamentos por transação relacionados ao uso da Wallet;
- Sem custos adicionais para PJ ou PF.
- Não conflita com as bandeiras de cartões de crédito.
- Preparado para evolução com Open Finance e JSR.
- Sem a necessidade de realização de cadastro ou ativações para os clientes.
- Wallet multiplataforma, interoperável e 100% nacional.
- Utilização dos instrumentos de segurança do Pix.
- Diferente da atualização TAP to Pay ou Cash da Apple, que vira a partir do IOS 18.1 e que rodará a partir do IPhone 11. O aplicativo instantâneo APP Clip, está disponível desde a versão IOS 15, onde rodará em todos os iPhone, posteriores a versão 7. Já o Instant APP do Android, está disponível desde a versão 6.0 (Marshmallow. Atualmente já estamos na versão 14)
- Criado por um amplo consórcio de empresas brasileiras que visam a democratização dos pagamentos contactless;
- Vanguardismo no desenvolvimento e apresentação de uma solução global para pagamentos por aproximação;

TAP2PIX.org

Teste agora mesmo o Tap2Pix com IOS

Utilizando Mercado Pago ou Itau

TAP2PIX.org

https://www.letsopen.com.br/p/principalidade-de-pagamentos

	Wallet Apple*	APP Apple NFC*	Wallet Google	TAP2PIX
Compatibilidade com QR Code	❌	❌	❌	✅
Compatibilidade com Link	❌	❌	❌	✅
Compatibilidade com NFC	✅	✅	✅	✅
Custo por Transação	+/- 1% do faturamento	+/- 1% do faturamento	ZERO	ZERO
Sistema Operacional Android	❌	❌	✅	✅
Sistema Operacional IOS	✅	✅	❌	✅
Jornada COM Redirecionamento	❌	❌	❌	✅
Jornada SEM Redirecionamento	✅	✅	✅	✅
BaaS e Bancos fora do OpF	❌	❌	❌	✅
TAPs COM Redirecionamento	❌	4 à 7 Taps	❌	4 à 6 Taps
TAPs SEM Redirecionamento	1 à 2 Taps	3 à 4 Taps	1 à 2 Taps	2 à 3 Taps
Transmissão no padrão EMV	✅	❌	❌	❌
Utilização em e-commerces	❌	✅	✅	✅
Biometria/FIDO Aliance	✅	✅	✅	✅
Transmissão do NFC via APDU	✅	✅	✅	❌***
Transmissão via Universal Link	❌	❌	❌	✅
Uso Instantâneo sem Instalação/ Configuração	❌	❌	❌	✅
Smartphones Apple	Iphone 11 / IOS 18.1	Iphone 11 / IOS 18.1	❌	Iphone 7 / IOS 15
Smartphones Android	❌	❌	Todos	Android 6.0 Marshmallow
Tempo Médio**	5 à 10 Seg	15 à 25 Seg	5 à 10 Seg	5 à 15 Seg

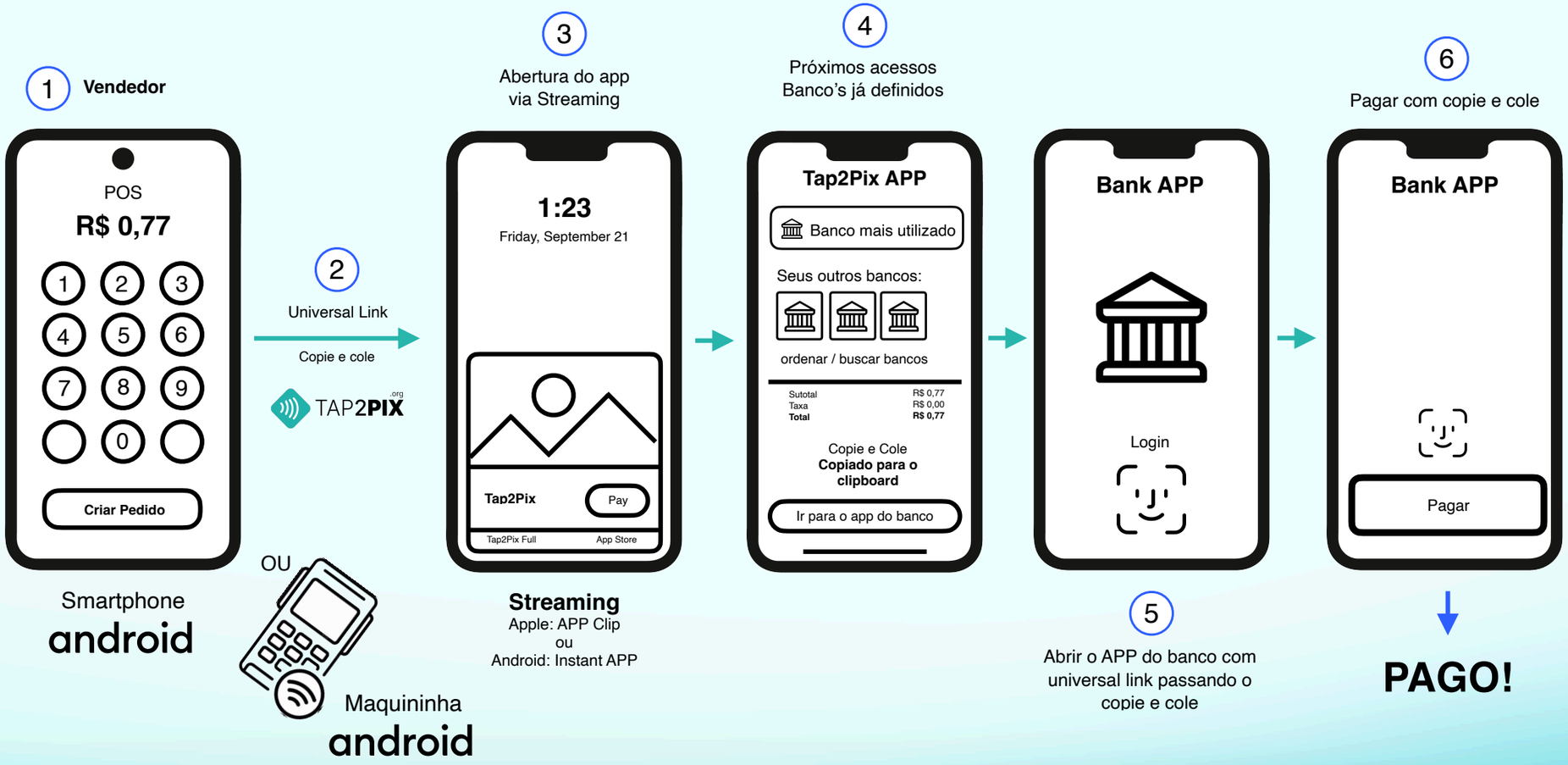
* Optamos em separar a Apple em 2 partes (Wallet Apple e Apple NFC), porque a Apple informou que permitirá aos desenvolvedores criarem uma possível wallet personalizada e concorrente ao Apple Wallet.

** O tempo médio no JSR, dependerá do acesso a APP da Iniciação, da conexão do PSP do Pagador e PSP do Recebedor. Enquanto o tempo médio do JCR, dependerá do redirecionamento para o APP e a conexão para o Pagamento.

*** Teria sim como usar a transmissão via APDU, porém ele se tornaria próximo ao APP Apple NFC, ou seja, perderia o propósito e necessitaria instalação e removeria diversos atributos, como: compatibilidade com QRCode, Link, Instantâneo…

TAP2PIX.org Wallet

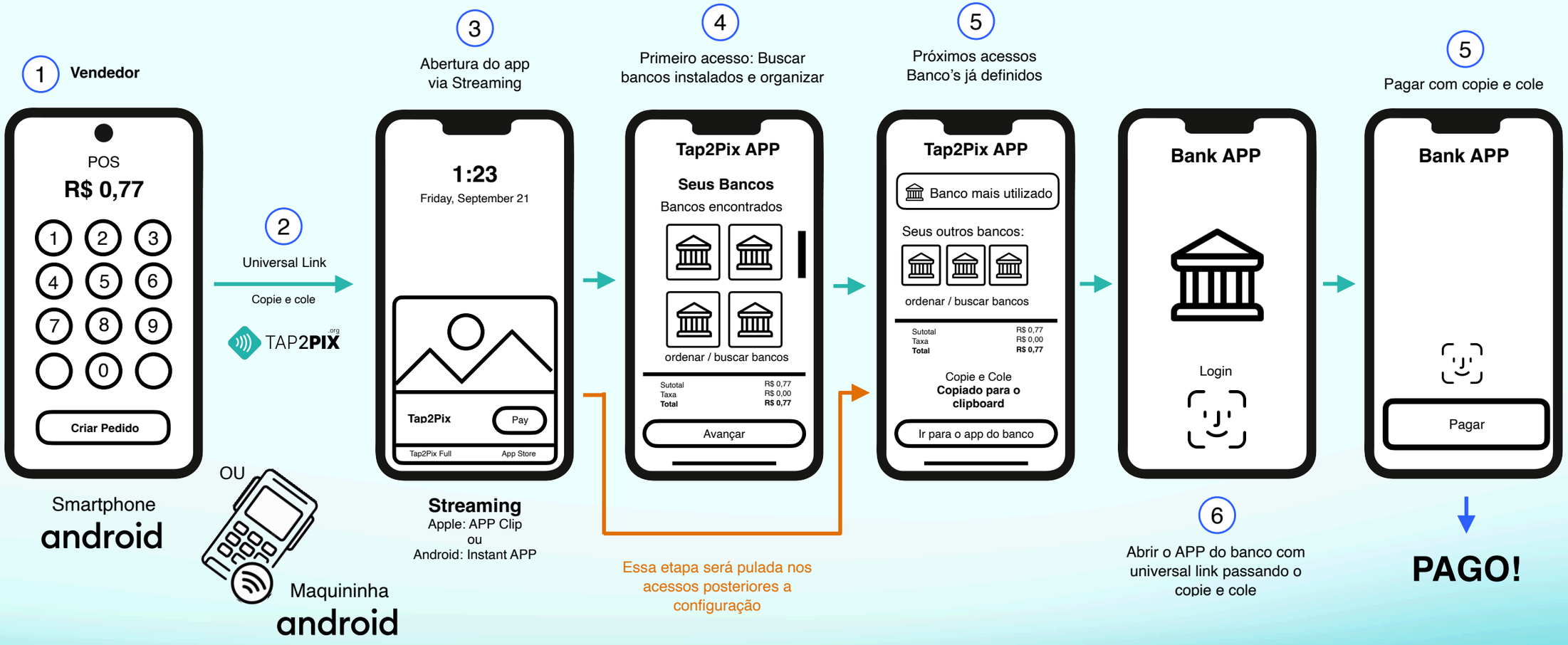
Jornada COM Redirecionamento Tap2Pix



TAP2PIX.org Wallet

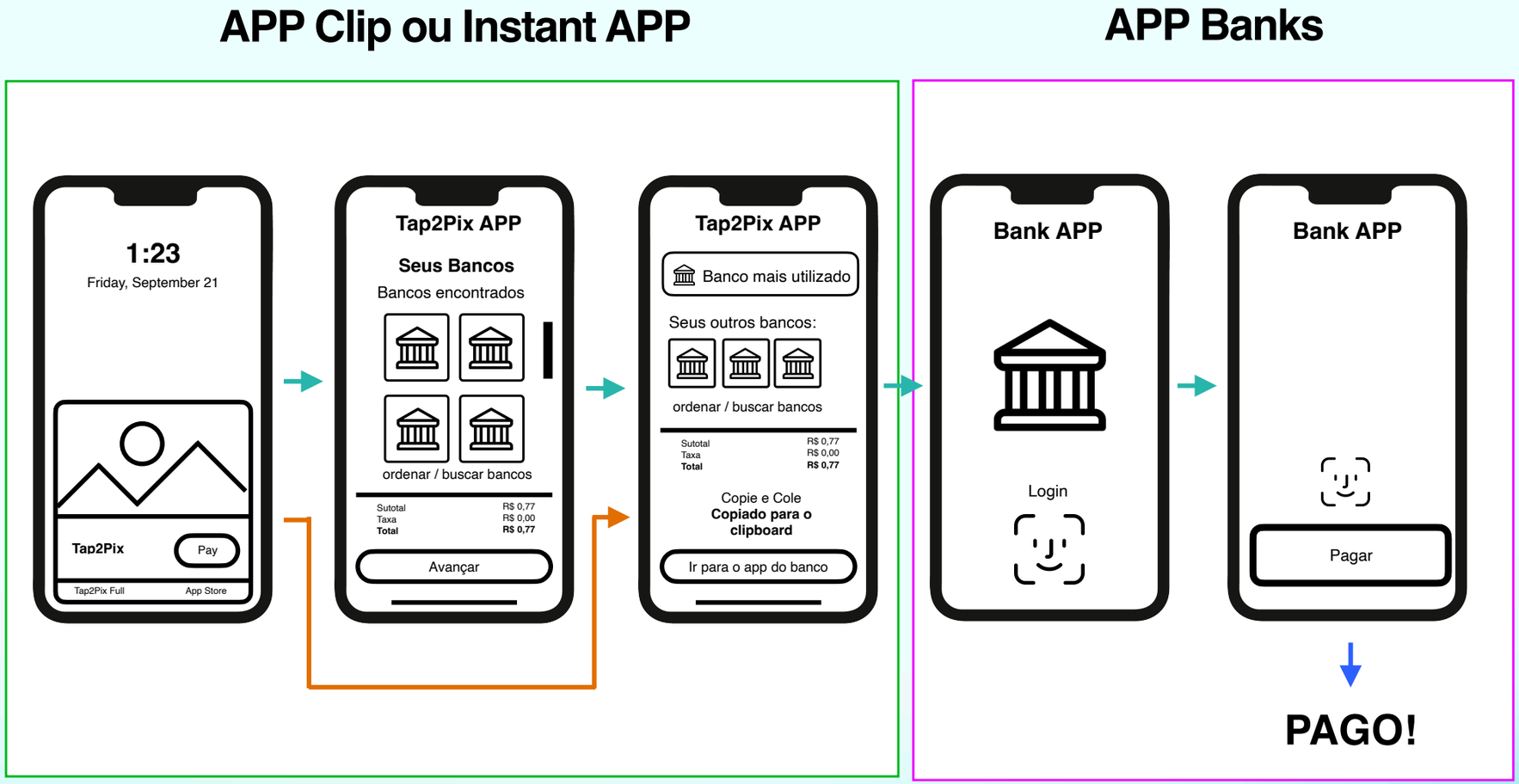
Jornada COM Redirecionamento Tap2Pix

com a ordenação dos bancos



TAP2PIX.org Wallet

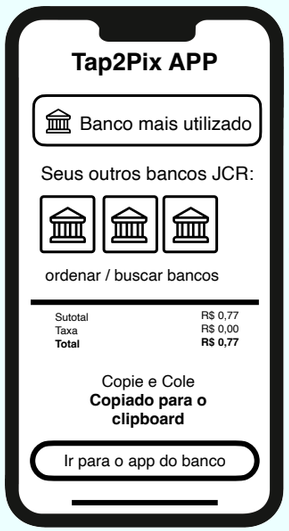
Jornada com Tap2Pix

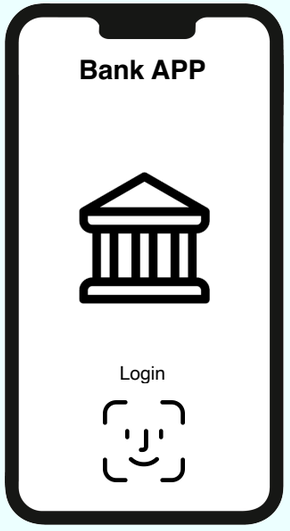


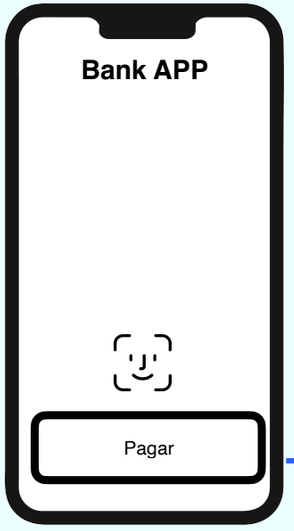
TAP2PIX .org
Wallet

JCR (Jornada COM Redirecionamento)

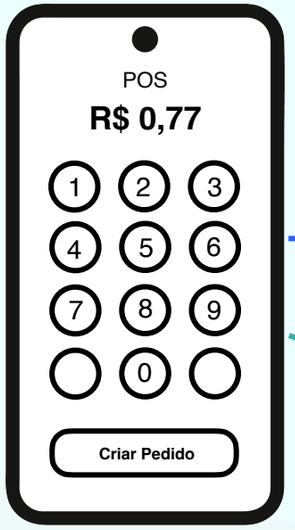
Streaming
Apple: APP Clip
ou
Android: Instant APP







PAGO!



Smartphone
android

https://tap2pix.org/copie&cole

OU

Maquininha
android

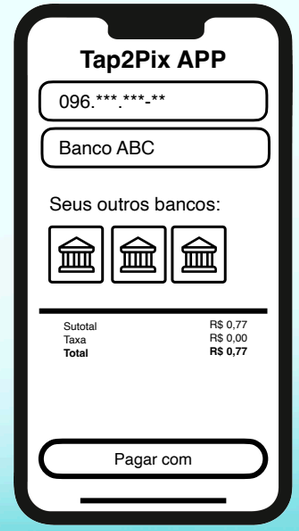
TAP2PIX .org

Proxy para UX

https://tap2pix.org/copie&cole

JSR (Jornada SEM Redirecionamento) & JCR (Jornada COM Redirecionamento)

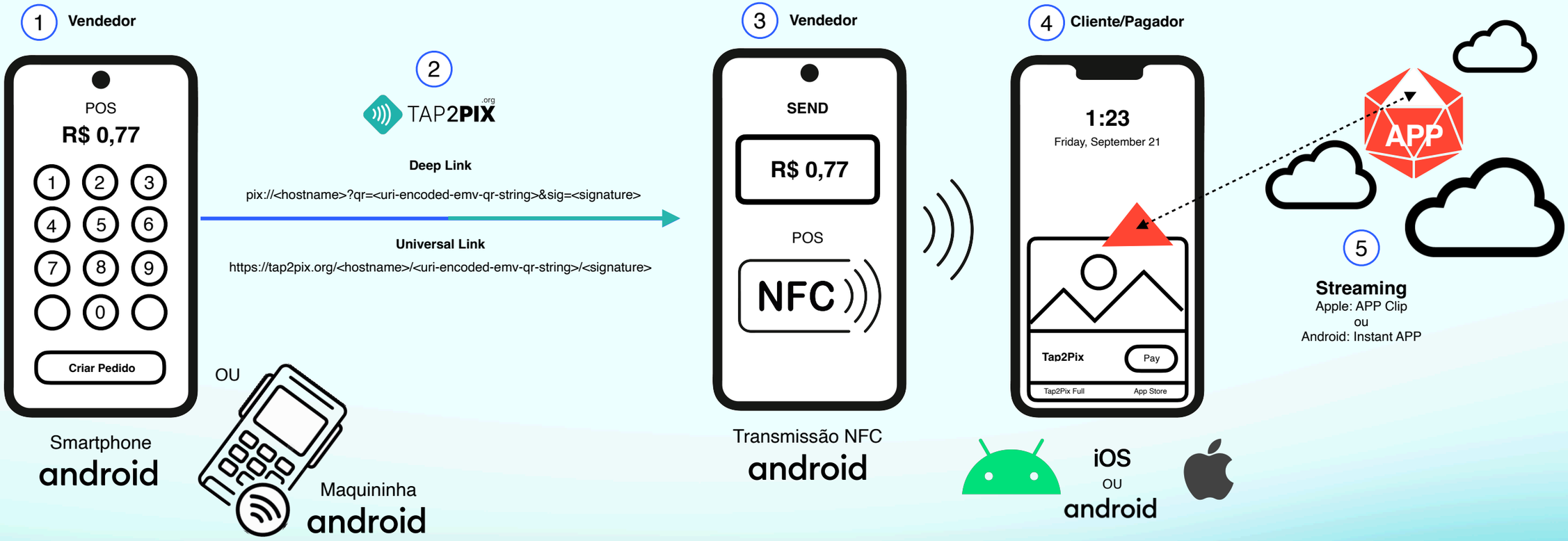
Streaming
Apple: APP Clip
ou
Android: Instant APP



PAGO!

Jornada com Tap2Pix

Pix por aproximação : **Utilizando o universal link para abrir o app streaming**



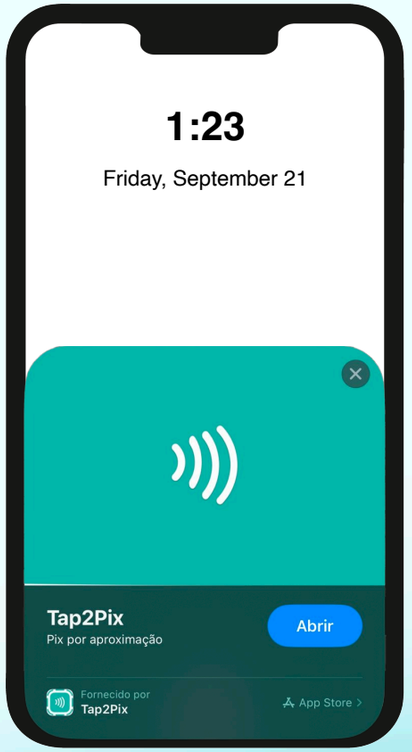
Tap2Pix o Super App Wallet!

O Projeto Tap2Pix não é apenas um aplicativo comum; ele é a materialização de um **Super APP Wallet**, disponível tanto para iOS quanto para Android. Ele representa a evolução no uso de QR Code, Links e NFC, facilitando a adaptação de clientes e instituições às jornadas de pagamento, com e sem redirecionamento. Além disso, o Tap2Pix abre novas oportunidades para todos os serviços BaaS e Bancos Sociais participarem do sistema Pix por aproximação.

Acreditamos que o Pix por aproximação deve ser uma propriedade 100% brasileira. Por isso, propomos uma associação que democratize sua governança, conferindo legitimidade e tornando-o acessível a todos os tipos de brasileiros.

É importante ressaltar que o formato de padronização proposto pelo Tap2Pix pode ser utilizado imediatamente, sem a necessidade de esperar pelo lançamento do JSR (Janeiro de 2025). Além disso, ele está em conformidade com todas as regulações e o mais alto padrão de segurança necessário.

TAP2PIX.org



Um padrão de pagamento por aproximação aberto para todos!