TAP2PIX.org

Um padrão de pagamento por aproximação aberto para todos

Estudo técnico

Entendendo o funcionamento técnico e suas limitações

Qual o formato mais seguro parta se utilizar o NFC?

TAP2PIX.org

Um padrão de pagamento por aproximação
aberto para todos

Entendendo o funcionamento técnico e suas limitações

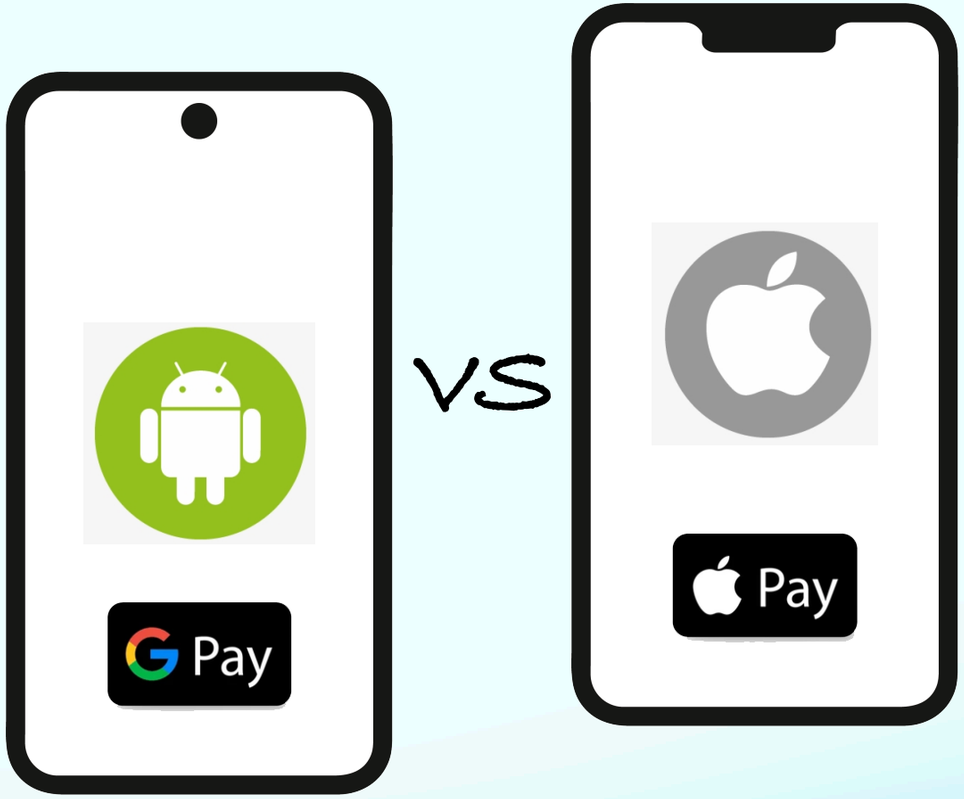
TAP2PIX.org

Secure Elements VS Cloud-Based HCE

Qual segurança é a melhor?

O **SE** (elemento seguro) baseado em hardware ou **HCE** (emulação de cartão host) baseada em nuvem?

De uma perspectiva de segurança, ambas as tecnologias concorrentes têm argumentos persuasivos a seu favor.

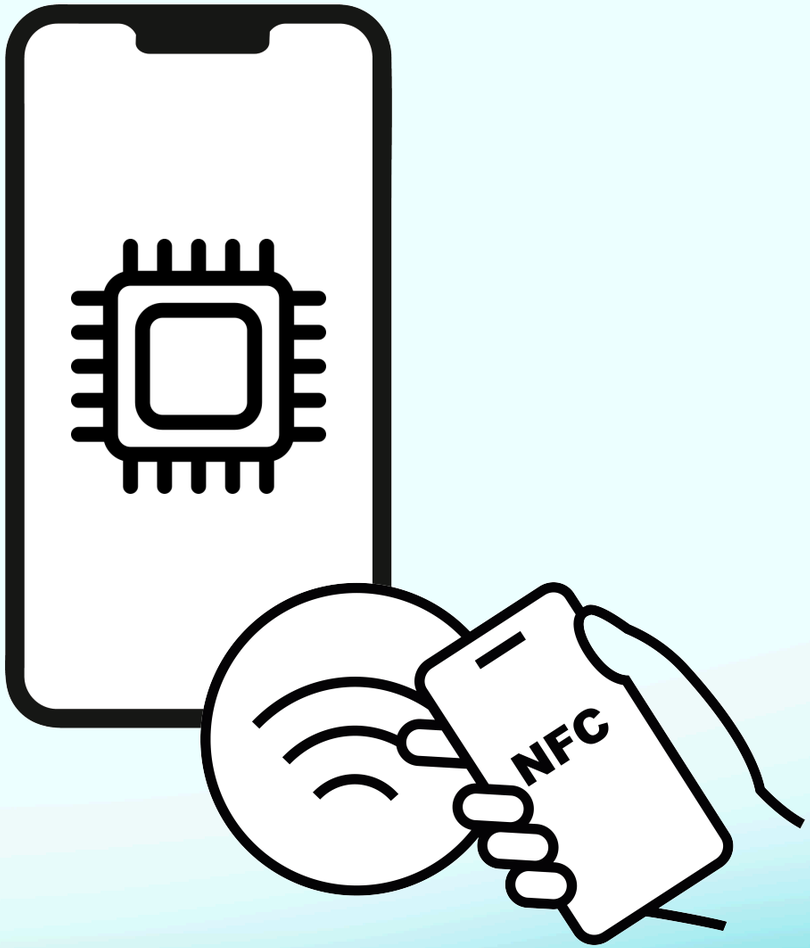


TAP2PIX .org

Secure Elements

Foram anos de dedicação para desenvolver uma solução de pagamento móvel confiável, baseada em elementos seguros (SE) altamente resistentes à adulteração. Estes elementos seguros, como os cartões inteligentes EMV, são isolados em telefones por uma interface de acesso restrita e criptografia forte, testados de acordo com requisitos das redes de pagamento para armazenar credenciais de forma segura. Com isso, a oportunidade de fraude é limitada a cada dispositivo, uma vez que apenas informações específicas do cliente e criptográficas são armazenadas nos SEs, diminuindo as chances de invasão por hackers.

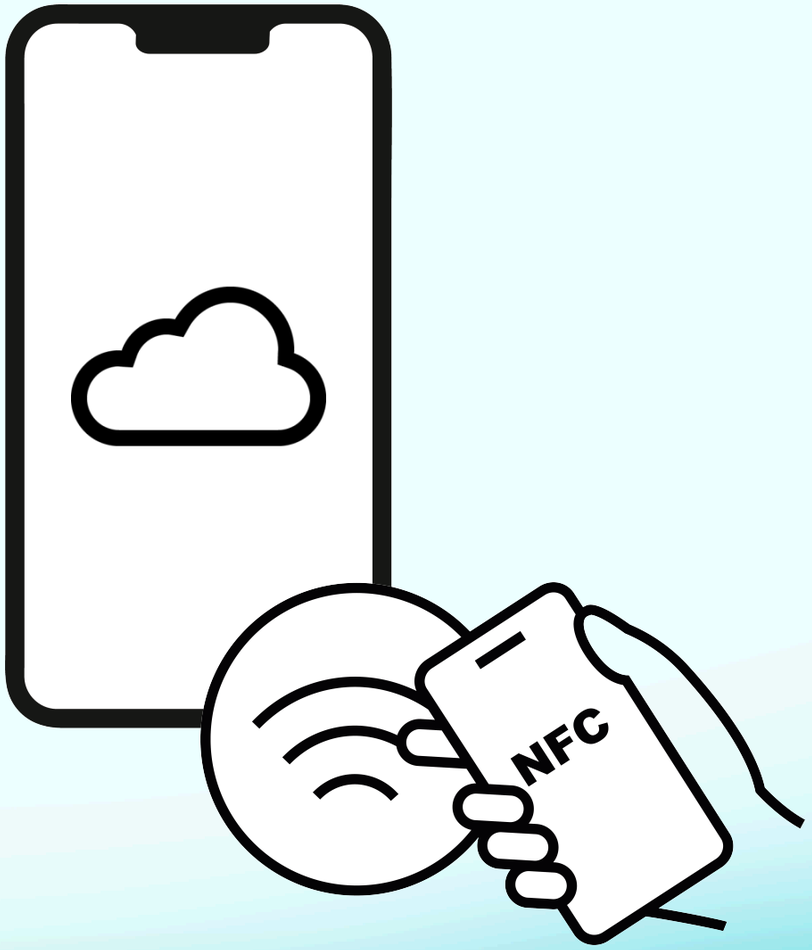
Esses elementos de segurança ganham destaque pela sua eficiência em manter os dados protegidos, garantindo a integridade das transações e restringindo a possibilidade de adulteração por terceiros. Assim, a confiabilidade dessas soluções de pagamento móvel é assegurada através de tecnologias avançadas e práticas de segurança, proporcionando aos usuários uma experiência segura e livre de preocupações com fraudes.



Cloud-Based HCE

A tecnologia HCE assume que dados armazenados em dispositivos são vulneráveis e, por isso, restringe o armazenamento de informações sensíveis para bancos de dados em nuvem com alto padrão de segurança. Os requisitos de segurança são extremamente rigorosos, ultrapassando padrões comuns e equivalentes aos de bureaus de personalização de cartões, considerando a concentração de informações de pagamento e credenciais como alvos atraentes.

A prevenção de acessos não autorizados no HCE é baseada em quatro pilares: chaves de uso limitado, tokens, impressão digital do dispositivo e análise de risco de transação. Essas medidas garantem a expiração rápida das chaves, a substituição do PAN por dados de uso limitado, a validação do dispositivo e a avaliação em tempo real de atividades suspeitas. A segurança do HCE depende do gerenciamento inteligente nos níveis de dispositivo e sistema, utilizando a constante conexão e análise de dados para uma segurança mais abrangente.

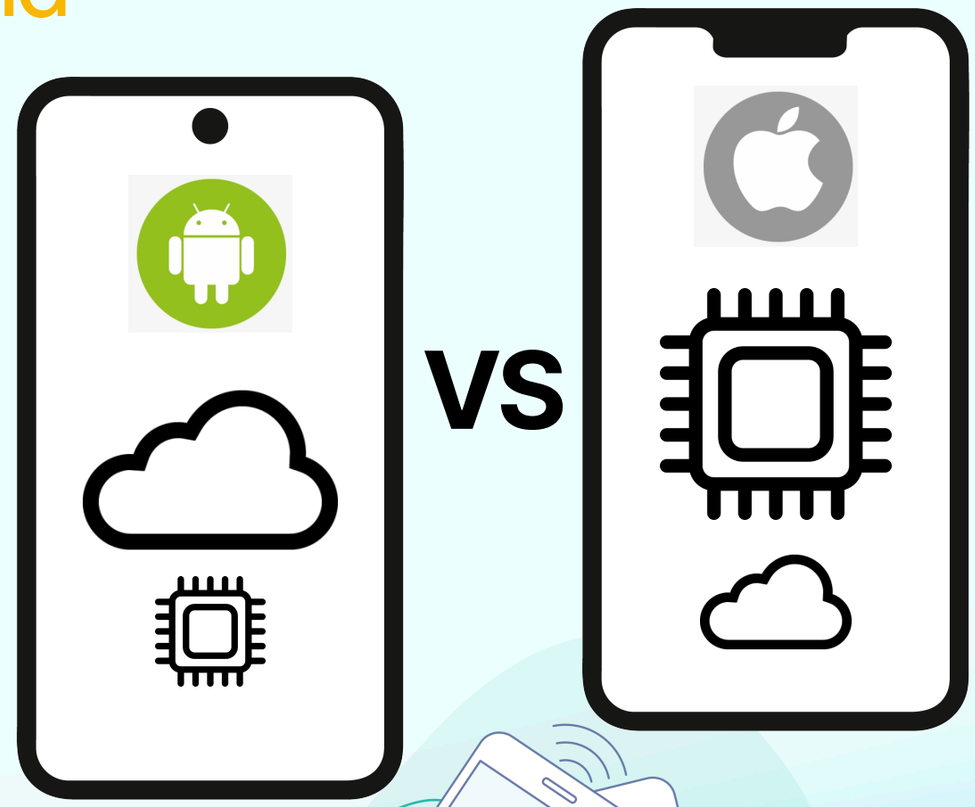


TAP2PIX .org

Diferenças entre Android e IOS

Hoje em dia vemos em ambas plataformas o uso do SE e HCE, porém por serem plataformas distintas, elas possuem políticas diferentes.

A plataforma do **Android/Google** é muito mais flexível e por ser uma arquitetura aberta e de diferentes fabricantes, assume a principal característica do HCE, onde considera que quaisquer dados armazenados em um aparelho são vulneráveis. Assim os dados de cartão de crédito nos aparelhos Android, dedica sua segurança no cloud. Muito similar a um HSM cloud.

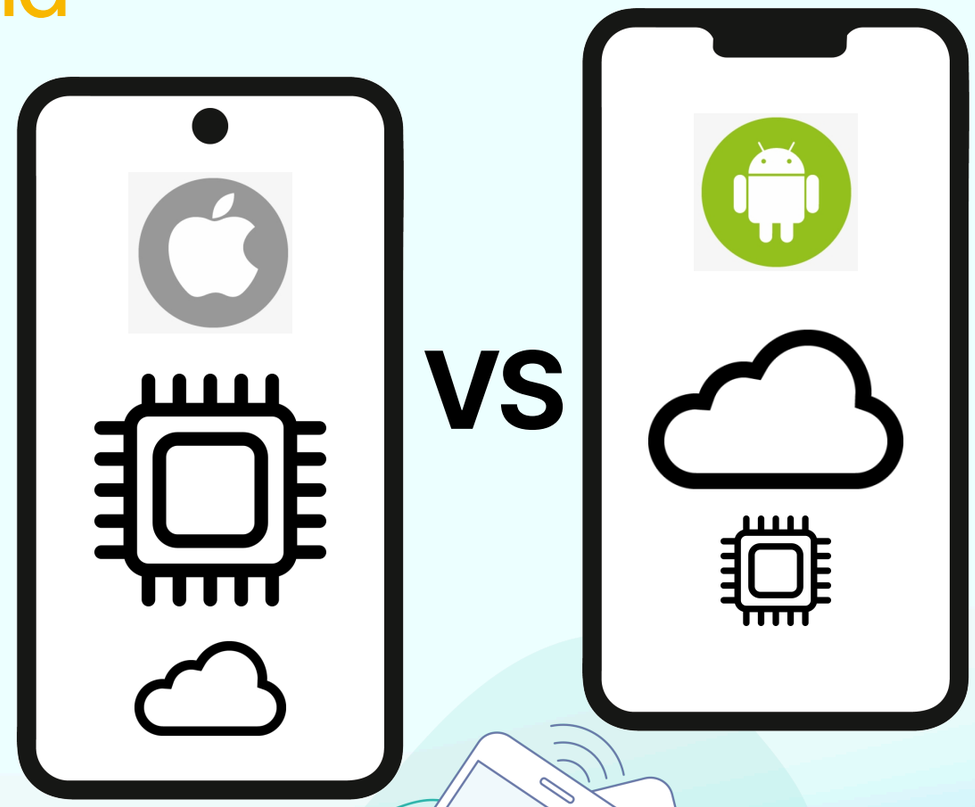


TAP2PIX .org

Diferenças entre Android e IOS

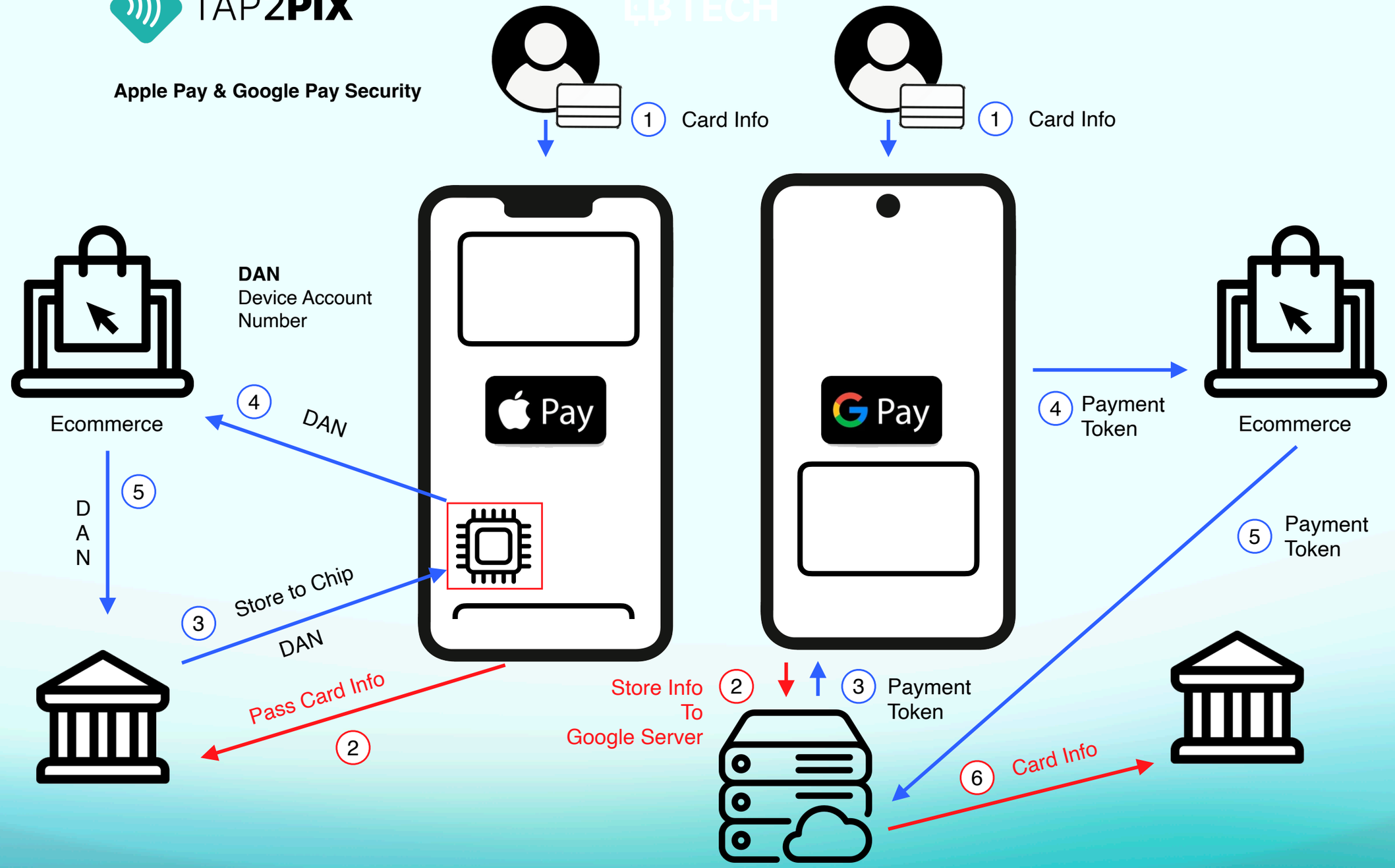
Por sua vez, o **IOS/Apple** demonstrou que aspectos do elemento seguro e da tecnologia HCE baseada em nuvem podem ser combinados em uma solução. O Apple Pay usa o elemento seguro para armazenar tokens e adiciona biometria com Touch ID ou Face ID para autenticação multifator.

Isso permite que a Apple use o poder dos dados locais e de backend para gerenciamento de risco, ao mesmo tempo em que remove todas as dúvidas sobre a segurança de um token ou credencial. Ao usar o melhor dos dois mundos, a Apple construiu um sistema forte.



TAP2PIX .org

Apple Pay & Google Pay Security



TAP2PIX.org

Comparativo

1. Suporte NFC
Android: Suporte amplo para leitura e gravação de etiquetas NFC, incluindo padrões como ISO/IEC 14443 (Tipo A e B) e ISO/IEC 15693. A maioria dos dispositivos Android permite a troca de dados entre dois dispositivos (NFC Peer-to-Peer) e a emulação de cartões.
IOS: Os iPhones suportam leitura de etiquetas NFC e, a partir do iPhone XS, leitura sem a necessidade de um aplicativo. O suporte para gravação de etiquetas NFC e emulação de cartões é mais limitado em comparação com Android, embora tenha melhorado com as versões mais recentes do iOS.

2. Capacidade das Etiquetas NFC
Android: Suporte para uma ampla gama de capacidades de memória, dependendo da etiqueta, incluindo até 64 KB com ISO/IEC 15693.
IOS: Capacidade de interação com etiquetas NFC com capacidades semelhantes, mas a funcionalidade é frequentemente baseada em aplicativos específicos que podem limitar o uso.

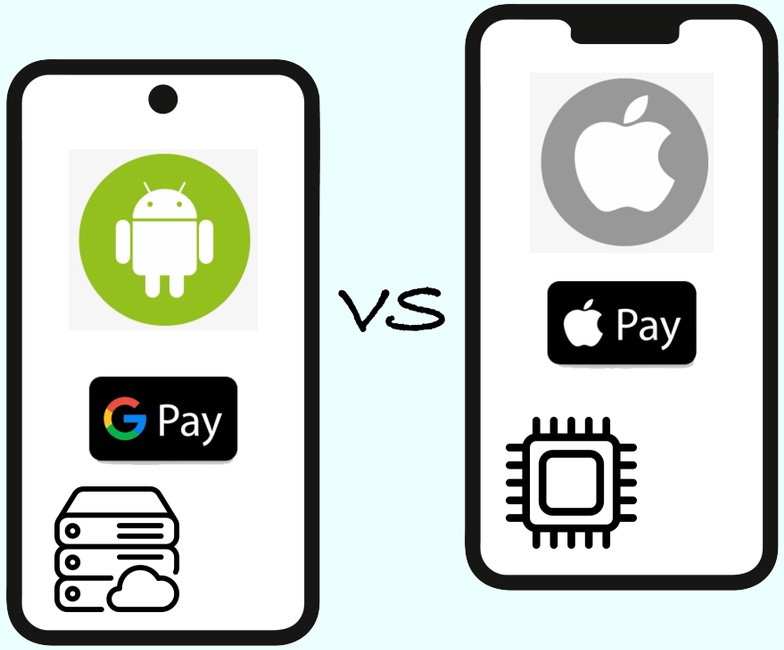
3. Aplicações de Uso
Android: Maior flexibilidade para desenvolvedores criarem aplicativos que utilizam NFC, incluindo uma variedade de funções, como pagamentos, transferência de arquivos e automação.
IOS: Integração mais restrita com o Apple Pay para pagamentos e algumas funções de automação, mas crescente suporte para leitura de etiquetas NFC em aplicativos específicos e a criação do APP Clip que possui interação com NFC e uma boa UX.

4. Interface do Usuário
Android: A interface pode variar amplamente entre diferentes dispositivos e fabricantes, resultando em diferentes experiências de uso de NFC.
IOS: Interface consistente em todos os dispositivos Apple, proporcionando uma experiência de usuário uniforme ao interagir com NFC.

5. Desenvolvimento, Carteira e wallet
Android: É muito flexível para o desenvolvimento de aplicativos com NFC. Dentre as personalizações temos seleção de wallet default e ampla variedade de leitura de NFCs.
IOS: Altamente restritivo ao uso dos NFCs, apresentando apenas recursos básicos e uma usabilidade um pouco melhor com APP Clip

TAP2PIX.org

Resultado



O SE (elemento seguro) da Apple é um exemplo de segurança de alto nível, baseado em hardware totalmente isolado e projetado especificamente para o Apple Pay. Isso resultou em um número extremamente baixo de vulnerabilidades e em nenhum caso de exposição dos dados de cartões dos clientes. Por outro lado, o Android não recomendo o uso do SE ou TEE (ambiente de execução confiável) devido à sua arquitetura aberta e dependência da segurança dos fabricantes. Em vez disso, o Android confia na tecnologia HCE (emulação de cartão host) baseada em nuvem para armazenar os dados de cartões dos clientes.

A diferença na abordagem de segurança entre a Apple e o Android é crucial quando se pensa no desenvolvimento de carteiras digitais, tanto para cartões de crédito, Pagamentos Instantâneos (Pix) ou criptomoedas.

Além disso, quando se trata da interoperabilidade e funcionamento das funções NFC entre plataformas, a confiabilidade da Apple supera a do Android. **No entanto, é essencial direcionar a atenção para o desenvolvimento de recursos NFC específicos para o IOS, considerando as restrições impostas pela Apple. Se um dispositivo NFC funciona com o IOS, é garantido que também funcione com o Android.**

TAP2PIX.org

Outras recomendações

É importante ressaltar a preocupação com as possíveis vulnerabilidades relacionadas ao SE (Secure Element) e ao TEE (Trusted Execution Environment) do Android. Ao longo desta apresentação, observamos que até mesmo o Google demonstra hesitação em confiar plenamente em sua arquitetura, que é aberta e depende da segurança implementada pelos fabricantes de smartphones. A tecnologia HCE (Host Card Emulation) foi desenvolvida como alternativa, para que os dados armazenados não fiquem em dispositivos físicos, por serem suscetíveis a riscos.

Diante dessa realidade, fiquei alarmado ao me deparar com projetos que utilizam a abstração de contas (RIP-7112) e fazem da criptografia de curva elíptica do TEE do Android para criar carteiras digitais em dispositivos móveis (conhecidas como, wallets para criptoativos).

Portanto, deixo aqui um alerta e uma recomendação para que se tenha cautela ao lidar com soluções de carteiras de ativos digitais, como criptomoedas, stablecoins e NFTs, que utilizam a curva elíptica da biometria para gerar chaves privadas alocadas no Android.

Para garantir a segurança dos ativos, é altamente recomendável o uso de cold wallets para armazenamento pessoal e custódia própria, e de HSMs (Módulos de Segurança de Hardware) para uso institucional. Estes dispositivos já possuem módulos dedicados para a criação de carteiras para criptoativos e certificações internacionais de segurança, garantindo assim um nível mais elevado de proteção e segurança.