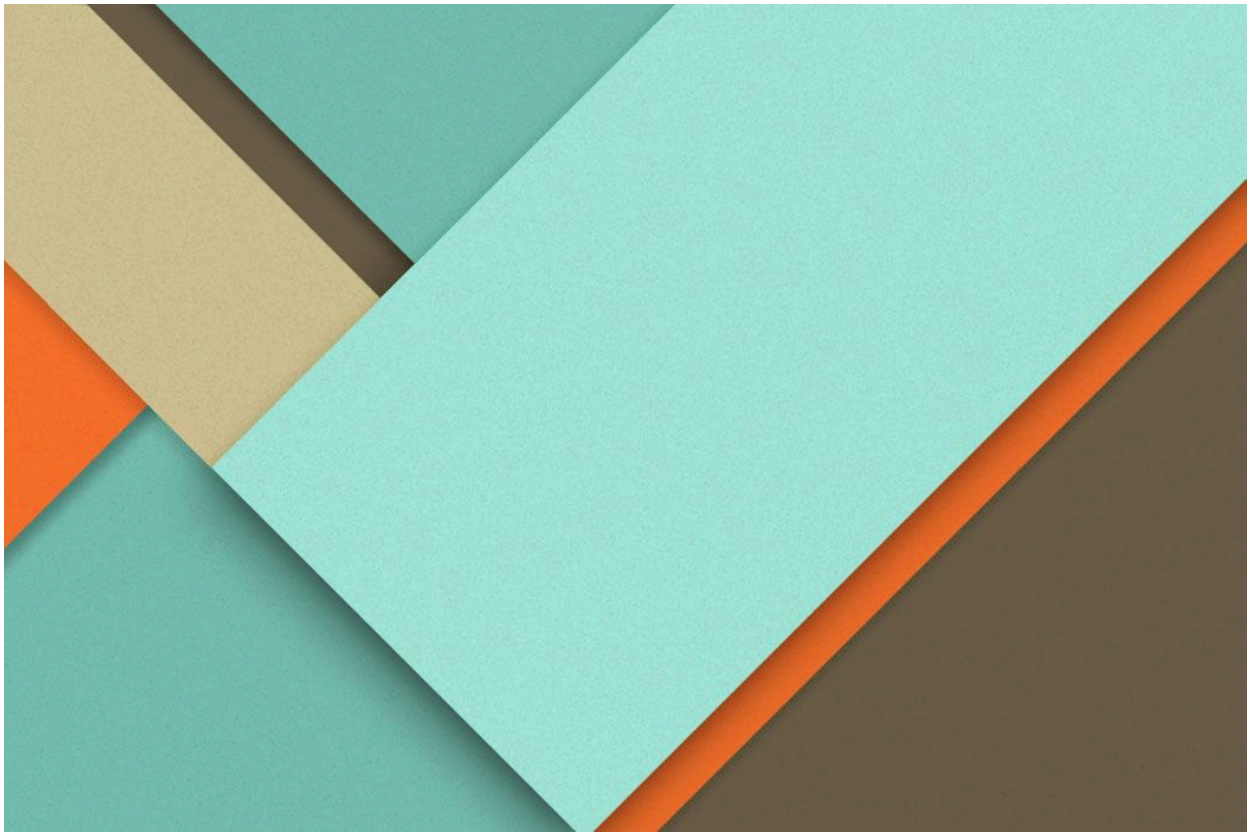

Resalvas e Inferências sobre o sistema de pagamento digital PIX

29.06.2025

Mario Caseiro
FAP Consulting em parceria com MCL Desenvolvimento de Software
Rua Galeazzo Alessi 70, conj 111
São Paulo, SP 04305-050

Overview

Retomada Técnica: Uma Camada Criptográfica de Integridade de Dados para Pagamentos Digitais

Introdução

O problema central abordado é a suscetibilidade de parâmetros sensíveis de transações expostos em requisições HTTP GET (*p.e.*, *Pix links de pagamentos*) à adulteração por agentes maliciosos, mesmo quando transportados por canais seguros TLS (Transport Layer Security) / SSL. O PKI (Public Key Infrastructure) tradicional autêntica primariamente a **identidade do servidor** e garante a confidencialidade e integridade do transporte, mas **não garante inerentemente a integridade dados em si**, se alterado antes da assinatura criptográfica ou após a descriptografia. A solução proposta implementa uma arquitetura criptográfica híbrida para estabelecer um modelo de uma nova entidade certificadora, no caso voltada para os dados chamada de DataTrust CA, garantindo a integridade dos dados de ponta a ponta para *links de pagamentos*.

Especificações

1. Canonicalização de Dados e Hashing SHA-256

- **O Problema** Os parâmetros GET brutos (*p.e.*, MARIO_CINTRA_LEITE_DE_OLI6009Sao_Paulo) são variáveis, concatenadas e potencialmente sujeitas a auterações.
- **Elemento de Solução: Algoritmo SHA-256:**
    - A *string atualmente canonicalizada dos links de pagamento pix* serviriam como entrada para a função *hash* de criptografia SHA-256 (Secure Hash Algorithm 256-bit).
    - **Funcionalidade:** SHA-256 é uma função matemática unidirecional que pega uma entrada de comprimento arbitrário (os dados canonicalizados) e produz um valor de *hash* de tamanho fixo de 256 bits (32 *bytes*), tipicamente representado como uma *string* hexadecimal de 64 caracteres (*p.e.*, 24be8e7f5e47e66618bafc16a7396e50c47e8088).
- **Propriedades da Criptografia:**
    - **Pre-image Resistance (Via Única,):** É computacionalmente inviável reverter a função *hash* para encontrar os dados de entrada originais a partir apenas do

valor de *hash*.
    - **Second Pre-image Resistance:** É computacionalmente inviável encontrar uma entrada diferente que produza o mesmo valor de *hash* de uma dada entrada.
    - **Collision Resistance:** É computacionalmente inviável encontrar duas entradas diferentes que produzem a mesma saída de *hash*.
- **Seu Papel na Solução:** O *hash* SHA-256 atua como um *fingerprint [impressão digital] criptográfica* única e inalterável dos dados da transação de pagamento original. Qualquer alteração, mesmo um único *bit*, nos dados canonicalizados originais resultará em um valor de *hash* SHA-256 completamente diferente.

2. DataTrust CA (PKI Extension para Integridade de Dados)

- **Conceito:** Baseando-se no PKI tradicional, o Banco Central estabelece um Central Bank CA Root de Pagamentos dedicado. Esta entidade certificadora CA é distinta das CAs que emitem certificados SSL/TLS para *web servers*, pois ela valida os Dados e não somente o transporte dos mesmo.
- **Funcionnalidade:**
    - Esta entidade certificadora CA emite *certificados digitais* para cada *link de pagamento* legítimo garantindo assim a fidedignidade do link gerado pelo sistema Pix. Estes não são *server certificates (certificados de servidores)*, mas sim *data validation certificates* (certificados de validação de dados) ou *certificados de autenticidade de links*.
    - Estes certificados contêm informações que ligam a URL de pagamento simplificada (que incorpora o *hash* SHA-256) ao Banco Central como o emissor confiável, e são criptograficamente assinados pela *chave privada* contida e mantida sob custódia da entidade certificadora CA Root de Pagamentos do Banco Central.
    - As instituições bancárias online participantes são pré-provisionadas com a *chave pública* deste novo CA Root de Pagamentos do Banco Central.
- **Seu Papel na solução:** Quando um banco online recebe um *link de pagamento* (*p.e.*, https://br.gov.pix/[HASH]), a primeira etapa de verificação envolve a validação criptográfica do *certificado digital* deste *link* contra o CA Root de Pagamentos do Banco Central. Isso previne o *spoofing de link* e confirma que o *link* foi **genuinamente emitido pelo Banco Central**.

3. Blockchain Anchoring (Immutable Ledger para Provas de Integridade)

- **Technology:** Um *permissionado blockchain* controlado pelo Banco Central.
- **Consensus de Algoritmos:** Ao contrário de *blockchains* públicas e descentralizadas que usam Proof-of-Work (PoW) ou Proof-of-Stake (PoS) para ampla confiança, *blockchains* permissionadas típicamente empregam algoritmos de consenso Byzantine Fault Tolerant (BFT) (*p.e.*, Practical Byzantine Fault Tolerance (PBFT) ou seus

derivados, Raft, consenso baseado em Tendermint). Estes algoritmos oferecem:
    - **Alto Throughput:** Significativamente mais transações por segundo do que cadeias PoW.
    - **Baixa Latência:** As transações são confirmadas rapidamente, frequentemente em segundos.
    - **Confiança Baseada em Identidade:** Os participantes (*nodes*) são conhecidos e autorizados, aumentando a segurança e a responsabilidade dentro da rede.
- **Papel na Solução:**
    - Para cada transação de pagamento válida, o *hash* SHA-256 calculado de seus parâmetros canonicalizados, juntamente com um UUID (Universally Unique Identifier) único para aquela transação específica, é submetido como uma transação para este *blockchain permissionado*.
    - O *blockchain* serve como um *imutável e distribuído livro de registros* que registra permanentemente ou temporariamente o *estado verificado* dos parâmetros (através de seu *hash*) para cada transação. Isso atua como a única e indiscutível fonte de verdade para o *original, sem adulteração na assinatura digital dos dados*.

4. O link seguro de pagamento e Processo de Verificação

Nova Estrutura de Link: A URL de pagamento Pix original e extremamente verboso, ou seja, dados sensíveis ficam a mostra, tendo parâmetros expostos, acabará sendo substituído por uma URL simplificada e segura do formato https://br.gov.pix/[SHA256_HASH]. Esta URI concisa funciona como uma referência direta à *prova de integridade imutável no blockchain*.

Workflow de Verificação nos Bancos Online:

1. **Link de Pagamento:** Um cidadão fornece o *link de pagamento* https://br.gov.pix/[HASH] através de seu sistema bancário *online*.
2. **Validação do Certificado:** O banco primeiro valida o certificado digital do domínio br.gov.pix contra a *chave pública* do CA Root de Pagamentos do Banco Central. Isso confirma a origem autêntica do *link*.
3. **Recuperação de Dados Originais:** O banco usa o *hash* SHA-256 incorporado (e potencialmente o *UUID da transação*) para consultar o sistema autorizador do Banco Central (que pode ser uma API) para recuperar os detalhes completos da transação original associados a esse *hash*.
4. **Re-Calculamento do Hash:** O banco então recalcula o *hash* SHA-256 desses detalhes da transação original recém-recuperados (após canonicalizá-los novamente, precisamente como estavam no momento da geração).
5. **Query no Blockchain:** Concomitantemente, o banco consulta o *blockchain permissionado* do Banco Central usando o *UUID* da transação (ou o próprio *hash* como um *index*) para recuperar o *hash* SHA-256 que foi originalmente ancorado no *blockchain* para esta transação específica e assim recuperar os dados que foram criptograficamente guardados no blockchain.

6. **Comparação de Integridade:** Uma correspondência criptográfica entre o *hash* recalculado e o *hash* recuperado do *blockchain* é a condição absoluta para a legitimidade.
7. **Decisão sobre a transação:**
    - **Match:** A transação é considerada legítima e prossegue.
    - **Não der Match:** Qualquer discrepância indica adulteração. A transação é imediatamente rejeitada e um alerta é acionado.

5. Implicações e Tecnologias Complementares:

- **Micro Serviços e MessagePack:** Conforme discutido, para uma troca de dados mais ampla entre *micro serviço*, a serialização de dados em formatos compactos e eficientes como MessagePack antes do *hashing* minimizaria o tamanho dos dados de entrada, otimizando ainda mais o desempenho do *hashing* e o armazenamento/throughput do *blockchain*. Este princípio estende o DataTrust CA além de apenas URLs.
- **Segurança em Camadas:** Esta arquitetura adiciona uma camada crucial de integridade de dados sobre a segurança de transporte existente (TLS/HTTPS) e a segurança em nível de aplicação, fechando efetivamente a lacuna onde os parâmetros poderiam ser alterados sem quebrar a sessão TLS como ocorre hoje em dia.
- **Infra Estrutura Física:** A visão de "alqueire data centers" sustenta fisicamente todo este *framework de segurança digital*, fornecendo o ambiente resiliente, de alta disponibilidade e fisicamente seguro necessário para uma infraestrutura nacional tão crítica (*servers*, *equipamentos de rede*, *sistemas redundantes de energia com andares dedicados a baterias e andares dedicados a geradores, para manter a continuidade dos serviços em operação*). Esta infraestrutura será abordada em documento à parte.

São Paulo, 12 de junho de 2025

MC LOC

gov.br
Documento assinado digitalmente
MARIO CINTRA LEITE DE OLIVEIRA CASEIRO
Data: 29/06/2025 13:02:07-0300
Verifique em https://validar.iti.gov.br