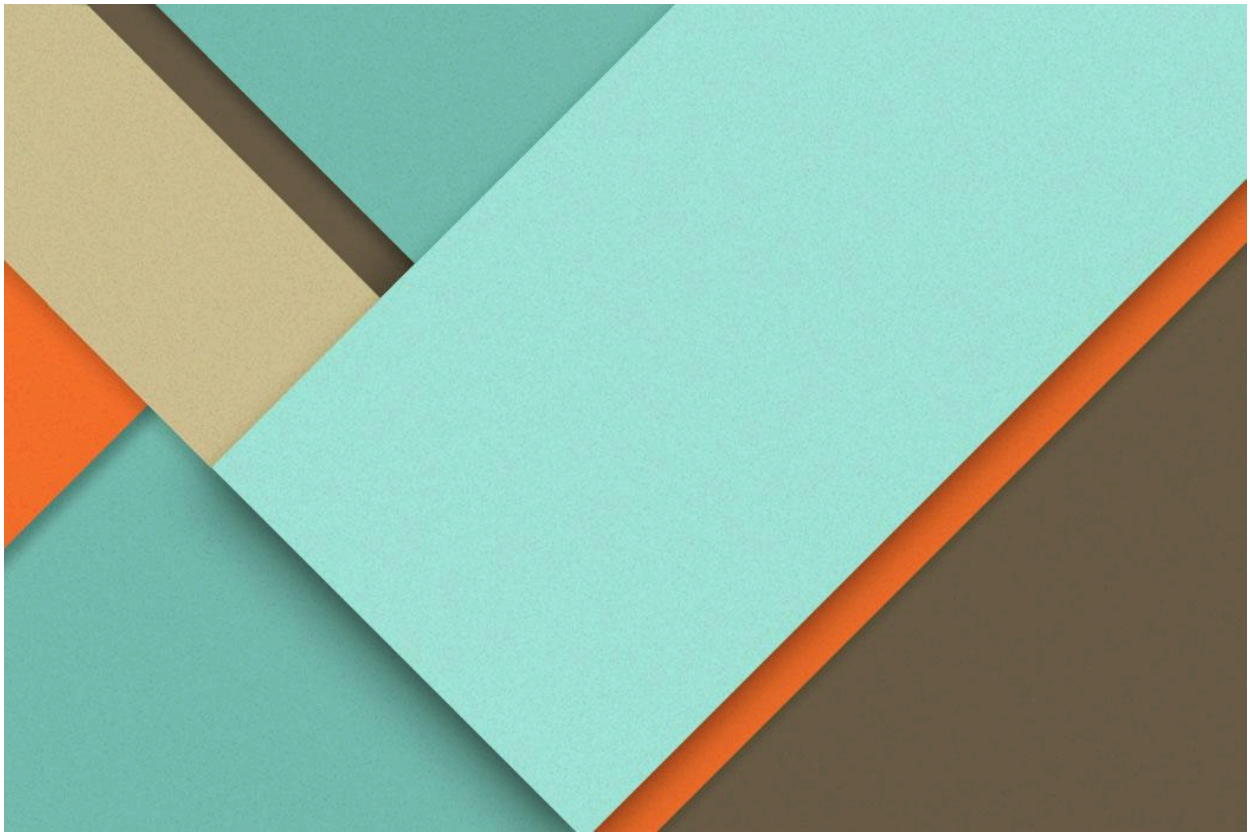

DataTrust CA, um novo conceito de autoridade em segurança da informação

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

Technical Brief: DataTrust CA para Integridade de Dados Nacionais - Uma Perspectiva de Arquitetura de Software

Introdução

Este documento descreve a arquitetura técnica e os princípios de criptografia que se destacam na proposta de criação de uma nova entidade certificadora, o DataTrust CA, uma camada crítica para garantir a integridade **dos dados** em infraestruturas digitais nacionais, como o sistema de pagamentos Pix. Esta iniciativa vai além da mera segurança de transporte (TLS/SSL) para garantir a fidedignidade e não corrompimento tanto quanto a autenticidade da origem dos *payloads* de dados na camada de aplicação do sistema financeiro nacional digital PIX.

Especificações

1. A natureza do DataTrust CA - um novo conceito de certificados: Para além da Segurança de Transporte

Embora o TLS garanta efetivamente o canal de comunicação criptografando dados em trânsito e autenticando identidades de servidores, ou seja, garante que você ou sua aplicação esteja realmente falando com quem imagina, ele [TSL/SSL] não protege realmente os dados contra a manipulação de parâmetros enviados e/ou recebidos antes de serem serializados e criptografados no lado do remetente, ou após serem descriptografados no lado do receptor. Esta vulnerabilidade, exemplificada pela adulteração de parâmetros URL GET, necessita de uma atestação/validação criptográfica da origem e integridade do conteúdo [dados] na camada de aplicação.

O DataTrust CA aborda isso estabelecendo um *framework* confiável onde o próprio conteúdo dos dados é criptograficamente assinado e verificável por um novo conceito de CA Root.

2. Conceito Criptográficos Essenciais

O DataTrust CA baseia-se na sinergia de dois conceito criptográficos fundamentais:

2.1. SHA-256 para Content Fingerprinting

- **Algoritmo:** SHA-256 (Secure Hash Algorithm 256-bit) é uma função *hash* criptográfica unidirecional. Ele aceita uma entrada binária [bytes, mesmo que ASCII] de comprimento arbitrário/aleatório e produz uma saída fixa de 256 bits (32 *bytes*) de tamanho, tipicamente representada como uma *string* hexadecimal de 64 caracteres.
- **Propriedades:** O SHA-256 é projetado para ser *collision-resistant* (computacionalmente inviável encontrar duas entradas diferentes que possa produzir o mesmo *hash* computado [64 caracteres]), *pré-image resistant* (computacionalmente inviável fazer engenharia reversa da entrada a partir do *hash* [64 caracteres]) - ou seja, uma vez computado o *hash* de um pacote de conteúdo qualquer, primeiro, qualquer desvio de conteúdo gerará outro *hash* completamente diferente do original, isso chama-se *pré-resistant;*

  Segundo, não é possível retroceder aos conteúdos originais através simplesmente do hash computado. Por isso a abordagem de utilizar tecnologia blockchain, que funcionaria como um *de-para* - hash vs dados originais.

- **Regra para Implementação:** Para o DataTrust, todos os campos de dados sensíveis de uma transação (*p.e.*, origem do gerador do link de pagamento, valores, nome do emissor, datas - mesmo que estes estejam canonicalizados) são primeiro submetidos a um processo de criptografia ECC entre o emissor do link de pagamento e o banco central através de certificado emitido pelo DataTrustCA. Este processo transforma os dados em uma sequência de *bytes* padronizada e conhecida como *hash* da transação que no caso seria SHA-256. Este hash serve como o *fingerprint* (impressão digital única) criptografada e imutável dos dados originais.

2.2. ECC para Assinaturas e Fidedignidade Digital

- **Algoritmo:** *Elliptic Curve Cryptography* (ECC) é uma criptografia de chave pública que usa a estrutura algébrica de curvas elípticas.
- **Por que ECC:** O ECC oferece níveis comparáveis de segurança ao RSA com tamanhos de chave e comprimentos de assinatura incrivelmente menores, resultando em cálculos mais rápidos, requisitos reduzidos para armazenamento e menor consumo de largura de banda - vantagens críticas para sistemas de alto volume e sensíveis ao desempenho como é o caso do sistema financeiro nacional PIX;
- **Regra de Implementação do DataTrust CA:**
  - **Gerenciamento das chaves:** O Banco Central (**atuando como DataTrust Root CA**) gera um par de chaves ECC seguras (*private key* SK_CA para assinatura, *public key* PK_CA para verificação), armazenado de forma segura dentro de um Hardware Security Module (HSM) em um ou mais datacenters seguros mantidos pelo banco central.

- **Assinatura dos Dados (Lado da Autoridade Emissora - por exemplo um banco emissor de um link de pagamento PIX):**
    1. Hoje os dados já são canonicalizados pelo banco emissor e validados pelo BACEN; Falta somente gerar um *hash* destes dados e validá-los no banco receptor tal hash com tecnologia blockchain;
    2. Para geração de *hash* único recomendamos a utilização de algoritmo SHA-256;
    3. Gerar uma *assinatura digital* ECC sobre o *hash gerado* usando a *private key* do DataTrust CA (*p.e.*., usando ECDSA).
    4. Criando assim um novo modelo de link verificável como por exemplo (https://br.gov.pix/[TRANSACTION_UUID]) ou

Novo modelo de link de pagamento pix:

https://br.gov.pix/8fec28102e0c371e6f2ecb949b95c1ba802260766b18c2445882b082418428b9

https://br.gov.pix/d1b592408180e1ac06390d0dab4f5844def1a9f4f356201fbed18f927cc2d033

https://br.gov.pix/ecd348dbaeb28d70c0a788d150b09e9acbd55f6e1808777d32827e3d2ee12072

Estes seriam exemplos dos novos links propostos para transações PIX em blockchain, somente este dado *hash 256* seria trafegado entre os utilizadores. É garantido via Criptografia ECC na blockchain do BACEN.

- **Verificação de Dados Data pela entidade Consumidora:**
    1. Receber o link de pagamento com seu hash somente, e nada mais de parâmetros, somente o *certificado* Cert_CA do DataTrust CA do emissor.
    2. Validar Cert_CA usando a conhecida *Central Bank DataTrust Root Public Key* PK_Root_CA (*validação padrão X.509 chain*, garantindo a autenticidade e o período de validade do certificado, recomendamos que este certificado que será gerado por cada link de pagamento tenha um tempo de expiração curto, descartando assim da infraestrutura de blockchain tanto o dados/parâmetros de pagamento como seu *hash* computado, além do par de chaves). Isso autentíca a origem do conteúdo;
    3. Computar o *hash* SHA-256 dos dados canonicalizados recebidos:
    4. Verificar a assinatura digital desta transação usando *hash computado* e a chave pública PK_CA do DataTrust CA (extraída de Cert_CA).
    5. **Verificação de Integridade Crítica:** Se hash calculado for igual ao *hash* original e a assinatura do certificado verificar com sucesso através do PK_CA, então tanto a autenticidade (assinada por CA confiável) quanto a integridade (conteúdo corresponde ao *hash* assinado) dos dados são confirmadas garantindo a fidedignidade da transação. Qualquer discrepância indica adulteração e a transação deverá ser descartada.

3. Integração com Blockchain: Atestado de Imutabilidade

- **Proposta:** O DataTrust CA baseia-se em uma Distributed Ledger Technology (DLT - tecnologia distribuída escalável) permissionada (*blockchain*) como um repositório imutável e à prova de adulteração para *hashes* autoritativos. Este repositório deverá ser construído e implementado e mantido sob a custódia do BACEN.
- **Mecanismo:** Para cada transação válida, um registro (*Transação_UUID*, *SHA256_Hash_of_Data*, *Timestamp*, *Emissor_ID*) é submetido ao *blockchain*.
- **Consenso:** Dada a exigência de alto *throughput* e alto desempenho em sistemas de pagamento, algoritmos de consenso para *blockchains* permissionadas (*p.e.*., PBFT ou protocolos similares derivados de BFT) são empregados, garantindo o acordo entre um conjunto conhecido de participantes autorizados sobre a ordem e validade das transações.
- **Papel da Verificação:** Quando uma entidade consumidora (FI) recebe um link de pagamento, após o cálculo de *hash* local e verificação de assinatura ECC, ela consulta o *blockchain* usando o *Transaction_UUID* para recuperar o *hash* SHA-256 originalmente registrado. Este *hash ancorado no blockchain* serve como a fonte definitiva de verdade e fidedignidade para comparação com o *hash* recalculado dos dados recebidos.

4. Considerações para Implementação do Software

- **Bibliotecas Criptográficas:** Seleção e integração de *cryptographic libraries* validadas por FIPS para SHA-256 e ECC.
- **Sistemas de Gerenciamento Chave (KMS):** Design e implementação de KMS seguros, resilientes e auditáveis para gerenciar *chaves privadas* do DataTrust CA assim como hoje são feitos nas chaves de cartões de chip de débito e crédito. Políticas de *rotacionamento de chaves* e recuperação de desastres para chaves são de suma importância.
- **SDKs/APIs para Serviços Clients:** Desenvolvimento de SDKs padronizados, seguros e de alto desempenho para que as entidades participantes integrem facilmente a lógica de assinatura e verificação do DataTrust CA. Isso inclui APIs para interação com o *blockchain*.
- **Performance e escalabilidade:** Otimização de operações de *hashing* e ECC para altos volumes de transações, como no caso do sistema financeiro nacional PIX. Implantação e dimensionamento de nós de *blockchain* para *throughput* máximo e baixa latência.
- **Postura em relação a segurança:** Implementação de autenticação multifator, *controle de acesso robusto*, *monitoramento contínuo* e *detecção de intrusão* para todos os componentes do DataTrust CA.

- **Auditoria e Governança:** Garantia de que todas as operações sejam auditáveis e

estejam em conformidade com as regulamentações financeiras e de segurança de dados sensíveis.

O DataTrust CA representa um salto crítico na confiança digital, passando de uma suposição de segurança de canal para uma garantia verificável de integridade do conteúdo, fundamental para a próxima geração de infraestrutura digital nacional segura.

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