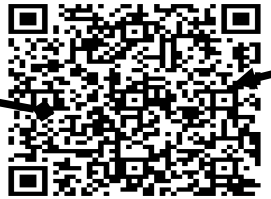
ProvTransaction

ProvMed

Aprovação de transações online baseada em tokens componente .



ProvTransaction

Dirigido a canais eletrônicos bancários para **aprovação de transações**:

→ Autenticação individual de transações associando tokens por transação a partir de uma semente.

→ gerador interno de componentes/sementes 100% baseado em software gerando milhões em horas com sementes de alto nível de alatoriedade sem custos.

ProvTransaction

ProvMed

Tipos de tokens: formação do código

1 OTP:

One
Time
Password

Semente:
FIXA
aleatória
imprevisível
criptografada

Tempo:
VARIÁVEL
Expira em 30s

=

código:
VARIÁVEL
muda a cada *30s*

2
Desafio resposta:

Semente:
FIXA
aleatória
imprevisível
criptografada

Tempo:
VARIÁVEL
Expira em 30s

desafio:
variável
aleatório

=

368448

Resposta:
VARIÁVEL
Depende do desafio

3
Assinatura eletrônica

Semente:
FIXA
aleatória
imprevisível
criptografada

Tempo:
VARIÁVEL
Expira em 30s

Transação:
VARIÁVEL

=

32376964

Asinatura:
VARIÁVEL
Depende dos dados da transação

oath
initiative for open authentication

ProvTransaction

ProvMed

Ameaças a soluções de tokens

Keyloggers: OTP pode ser capturado e reutilizado em transações falsas na janela de tempo de 30s.

Roubo de sementes de tokens armazenadas sem proteção em bases de dados SQL acessáveis por DBAs podem ser expostas através de ataques de engenharia social.

Ataques ao servidor de validação: aplicação de validação de códigos gerados incluindo lógica operacional e rotina criptográfica pode ser corrompida e substituída total ou parcialmente nos servidores de aplicação.

Vazamento de dados: Dados de transações podem ser capturados em tokens App de assinatura eletrônica antes da visualização.

ProvTransaction

ProvMed

Tokens desafio/resposta multi-sementes validados em repositório de componentes

Banco de tokens componente: Redis database

python™ powered

Object

Sementes múltiplas

Componente token:

OATH:
Public
Open
Market share

OCRA

oath
initiative for open authentication

ProvTransaction

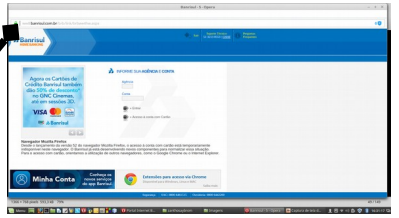
ProvMed

2 desafios 1 resposta por transação

RESPOSTA

97914586

Internet Banking

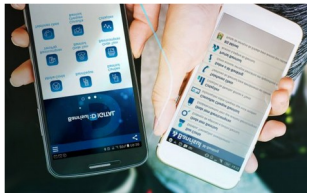


ATM

DESAFIOS

1 - valor aleatório #

2-# serial do objeto



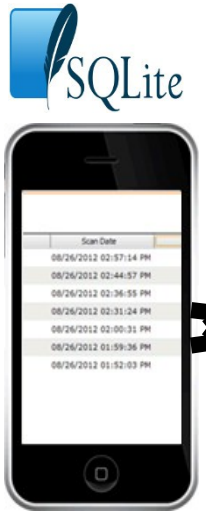
Mobile Banking

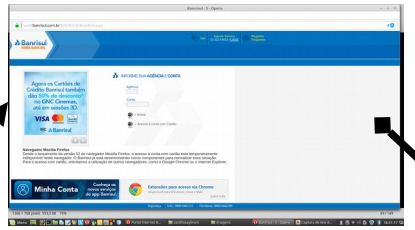
QRcode criptografado - **AES**

ProvTransaction

ProvMed

Elementos da arquitetura





Internet Banking

Roteador de canais

ATM

Mobile Banking

Tornado

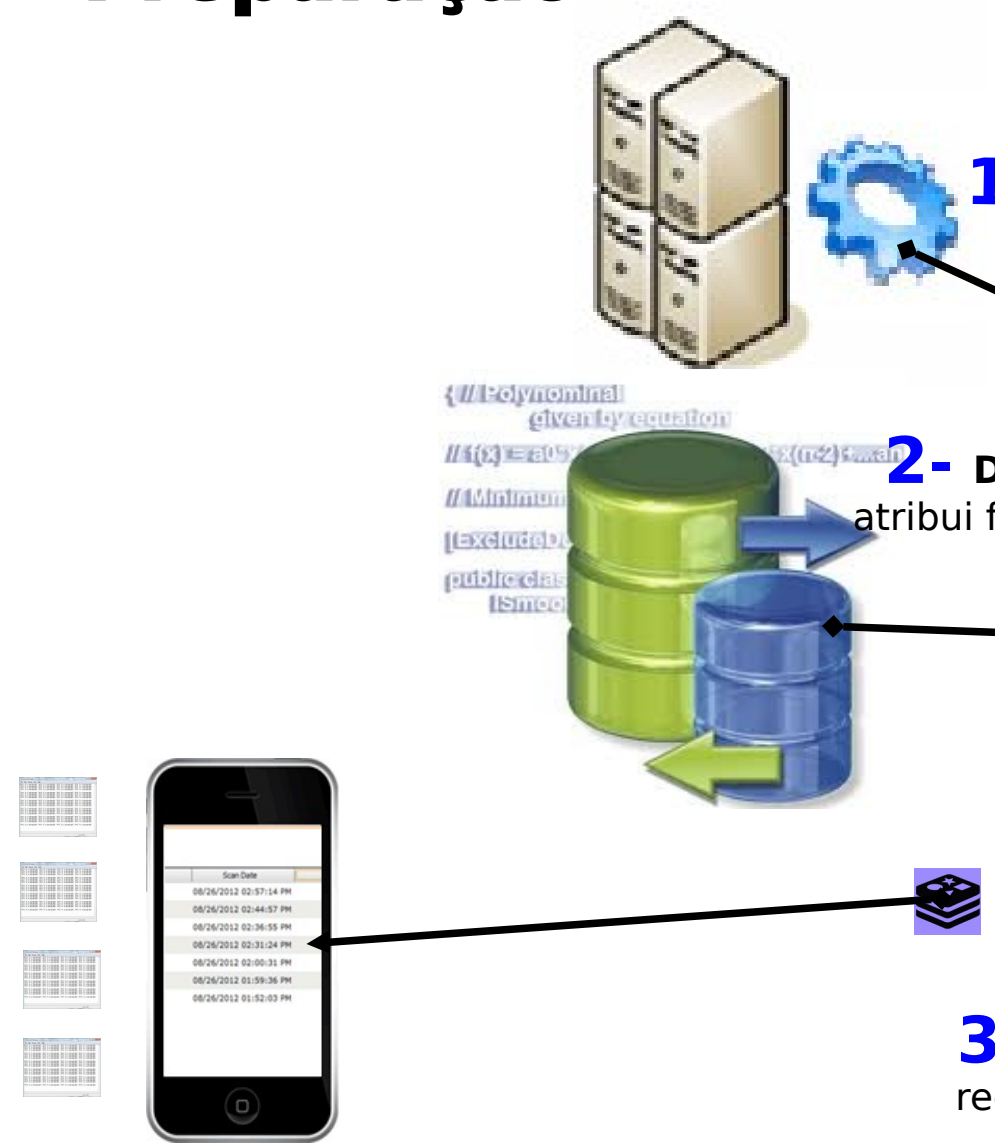
Tornado:
Webservice
REST

oath
initiative for open authentication

redis
database

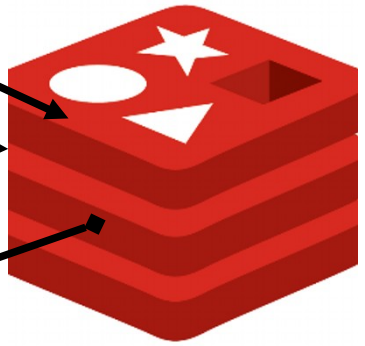
ProvTransaction

Preparação



1- Kickoff: Geração de objetos tokens.

2- Distribuição: banco atribui faixas de tokens por usuário baseado no consumo histórico



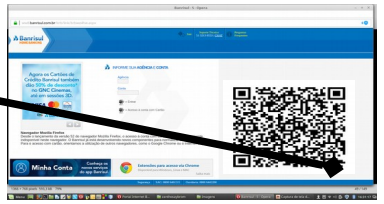
redis
database

3- Ativação: smartphone recebe a sua faixa de tokens

ProvTransaction

Uso

1-Desafios: O canal online apresenta um Qrcode incluindo um valor aleatório de sessão e o número serial de um objeto escolhido do usuário



2- Resposta: App lê o Qrcode gerando código de aprovação usando o objeto token selecionado.

3-: **Aprovação**::Após o código ser digitado e submetido no canal é validado diretamente no banco de dados de objetos

redis

database

ProvTransaction

Destaques

Leve: o uso de componentes de tokens armazenados em banco de dados noSQL exclui a necessidade de uma aplicação a parte de validação tornando banco de dados o validador com processamento distribuído nos registros fora do servidor de aplicações

Veloz: O uso de um banco de dados *noSQL residente em memória* acessado através de um servidor de aplicações de *atendimento assíncrono* proporciona grande performance e disponibilidade

Baixo custo: a plataforma gera suas próprias sementes encapsuladas em cada componente de token eliminando a necessidade do banco de licenciar por usuário.

seguro: QRcode criptografado e códigos de aprovação por transação eliminam eficácia de Keyloggers e base de dados independente acessado via programação eliminando extração por DBAs *não trafegando dados da transação*

Padronizado: o uso de OATH em modo desafio/resposta permite converter a solução para OTP e assinatura eletrônica visando mais conforto ou maior nível de segurança.