W3C – Web Payments

VICTOR THOMAZETTI MACHADO SILVA [ITAÚ]
GUSTAVO KOK [NETFLIX]

March 28th, 2023
AGENDA:

Brazil | Itaú | Victor | Gustavo

PIX Overview

Context:

  FIDO
  WEB
  LGPD/GDPR/PRIVACY

Challenges

  WEB P2M
  WEB CORPORATE
Brazil | Itaú | Victor | Gustavo

**Brazil**
- 214MM people
- Modern banking ecosystem
- Challenging fraud landscape ("Brazil is not for amateurs")
- 5 FIFA World Cup titles

**Itaú**
- Largest bank in LatAm
- 70MM customers
- USD 475 Bn in assets
- 40.9MM credit cards
- 34.5MM debit cards
- Official sponsor of the Brazilian soccer team

**Victor**
- 13 Years in Banking & Payments
  - 7 Years at Citibank
  - 3 years at ELO (Brazilian Card Scheme)
  - 3 Years at Itaú
- Member of several risk committees in Brazil (Card ecosystem, Open Banking, Instant Payments)
- Zero FIFA World Cup titles

**Gustavo**
- 8 Years of Payments / Payments Fraud
  - 3 Years at Dafiti Group
  - 5 years at Netflix
- Former member of card risk committee in Brazil
- Member of US Faster Payments Council Fraud WG
- Zero FIFA World Cup titles
PIX Timeline

2018
In May, a Working Group on Instant Payments, where Pix was outlined together with market players, starts to meet. Today, it is known as the Pix Forum.

2019
BC announcement on Open Banking.

2020
Pix is officially announced at the beginning of the year and goes live in November.

2021
Central Bank launches the Payment Initiator feature, in which it is possible to make a payment with Pix without having to access the bank’s app, Pix Seque and others.

2022 em diante
Pix Collection, Automatic Debit on Pix, Pix Guaranteed, Pix International, payment API, contactless payments, facial recognition payments, bluetooth payments, among other technologies.

Source: Image from labsnews.com
Pix – Brazil Instant Payment

**Concept**
- **real-time fund transfers**, available 24/7/365, without intermediation
- **costs**
  the absence of financial intermediation reduces the transactional cost structure
- **easiness**
  funds available in a few seconds, 24/7/365.
- **inclusion**
  allows payments of any type and amount between any party (IND/CO/GOV)
- **competition**
  flexible and open structure

**Simple**
Different ways to engage with a payment:
- QR code (static, dynamic, pagador)
- Key (Personal Tax ID, Corporate Tax ID, Mobile Number, Email, Random Hash)
- NFC
- Ability to schedule
- PIX link

**Good for payers**
- Fast
- Low cost
- Safe
- Simple

**Good for receivers**
- Lower acceptance cost
- Immediate availability of funds
- Payment automation and reconciliation
- Quick checkout experience

**Good for the market**
- Digitalization
- Financial inclusion
- More competition
Pix – Brazil Instant Payment - Scheme

Payer → OPF - AISP → Indirect part. → DICT + SPI (Central Bank) → Direct part. → Receiver

Receiver → Indirect part. → OPF - PISP → Direct part. → Payer
Pix – Big Numbers - # Keys/Id's

Source: Brazil Central Bank
Pix – Big Numbers - # Single Users

Source: Brazil Central Bank
Pix – Big Numbers - # Accounts

Source: Brazil Central Bank
Pix – Big Numbers - # Txn’s (‘000)

Source: Brazil Central Bank

27/03/2023
Pix – Big Numbers - $ Amount transacted

Source: Brazil Central Bank

27/03/2023
Pix – Big Numbers - Volume mix, per type

Source: Brazil Central Bank
Pix – Big Numbers - $ mix, per type

Source: Brazil Central Bank
Pix – Big Numbers - # Active users

Source: Brazil Central Bank
Pix – All numbers are public

## Pix – Brazil Instant Payment – Risk Overview

### Attractiveness
- Immediacy and 24x7x365
- Real-time gross settlement (RTGS)
- Similar transfer limits to other less popular payment types
- Processing and settlement model centralized at the Central Bank (single point of failure)
- Lack of knowledge of the end customer
- Lack of risk management knowledge of Indirect PSPs and payment initiators
- Public payment ‘keys’ (Email and Mobile)
- Payment ‘keys’ portability and claim process
- Absence of security capability of the payments system arranger

### Fraud Attacks
- Account hacking and transfer between multiple accounts on different PSPs with 24x7x365 withdrawal
- High-value transfers on non-working days / non-working hours
- Brute force attacks (DDoS) against the Central Bank and PSP’s connected to the ecosystem
- Social engineering and phishing to obtain payment credentials
- Opening of mule accounts in PSP’s that lack proper KYC processes
- Theft/transfer using ‘keys’ under the same ownership
- Creating new keys with newly/daily created emails and cell phones
- “Lightning kidnapping”, where people are forced to wire out their money. Targeted on non-working days and hours

### Mitigators
- 24x7x365 fraud prevention operation
- Real-time monitoring using machine learning models with the possibility of delaying and denying suspicious transactions
- Definition of maximum exposure limits based on risk criteria
- Safety education campaign for customers
- Strong authentication process on join and transaction (MFA)
- Strong evaluation process for indirect PSP’s to adhere to the arrangement, and strict fraud monitoring by sponsor
- Centralized market database to help validate credentials
- Fraud Risk Committe sponsored by the Central Bank to develop security features with key market stakeholders
## Context

<table>
<thead>
<tr>
<th><strong>LGPD/GDPR</strong></th>
<th><strong>FIDO</strong></th>
<th><strong>WEB</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Current general understanding is that, for fraud prevention purposes, we have a legitimate interest in the collection and use of personal information.</td>
<td>Itaú already using FIDO for some app-focused solutions.</td>
<td>Low level of confidence in the WEB channel due to several different types of attacks.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>CORPORATE</strong></th>
<th><strong>HARD-TOKENS/YUBIKEYS</strong></th>
<th><strong>BCB SECURITY GOVERNANCE</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Countless bank as a service initiatives are surfacing and we have the need to authenticate individuals in non-proprietary channels.</td>
<td>We already use hard tokens for corporate customers. We would like to stop using it, but can we?</td>
<td>We have a permanent fraud prevention strategy committee in conjunction with the regulator to address the evolution of security protocols in PIX and Open Finance.</td>
</tr>
</tbody>
</table>

27/03/2023
Hypothesis

Can we use SPC and FIDO2 to enable security for PIX P2M WEB transactions in Brazil?

Can we use SPC and FIDO2 to enable security for PIX corporate WEB/BaaS channels transactions in Brazil?
Thank You

Q&A