



# Attack on the Brazilian Financial System

How to Protect Privileged Access  
in Your Organization.



# What is the National Financial System?

The **National Financial System (SFN)** is the infrastructure responsible for enabling the circulation of money, credit and payments in Brazil, involving the Central Bank, banks, fintechs, cooperatives, payment institutions and key technology providers - such as PSTIs (IT service providers).

Through the SPB (Brazilians Payment System) and the Instant Payments System (SPI), the SFN guarantees the fast, secure and traceable settlement of transfers between institutions, thus supporting trust and the functioning of the financial market.

## Structure of the National Financial System

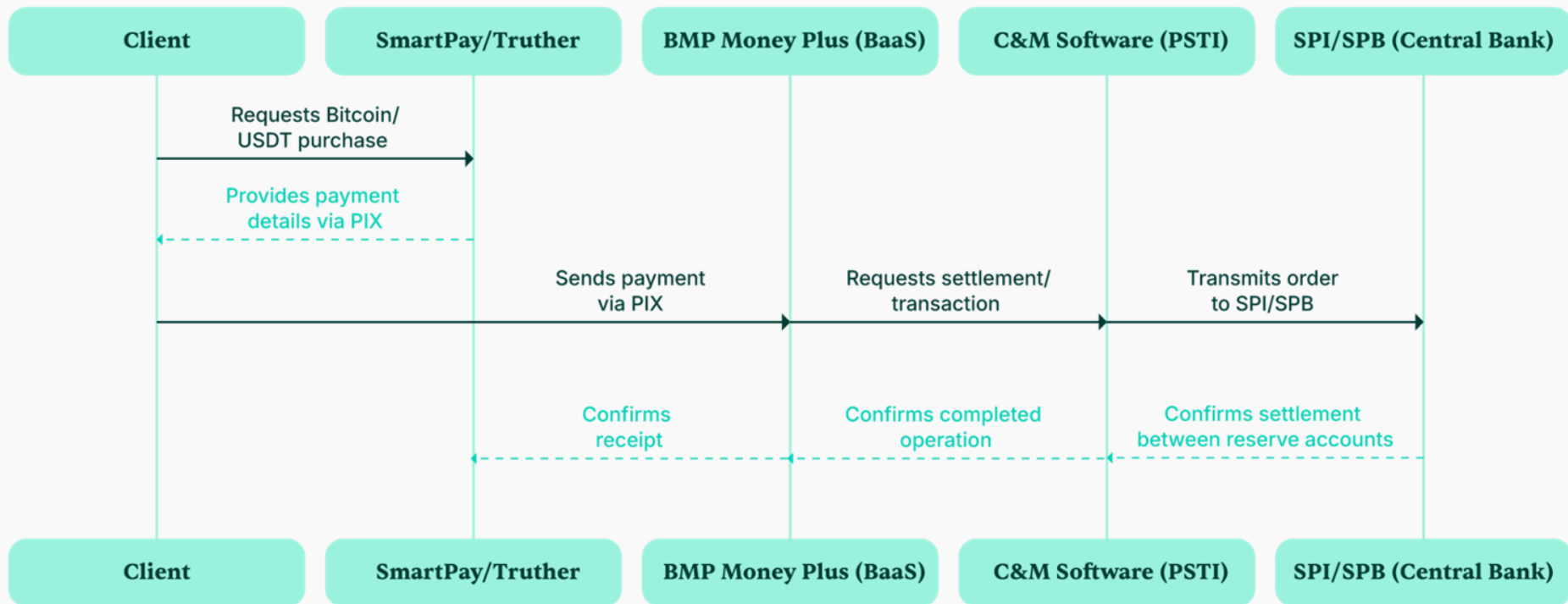
The SPB/SPI links financial institutions to the central bank.

To operate, these institutions require valid digital certificates and are supported by service providers such as C&M Software.

A weak link in this chain puts everyone at risk.

# Crypto Purchase Flow via PIX

SFN steps to convert Pix into cryptocurrency



## Suspicious transfer: The Early Warning.

**4:00 AM**

At 4 a.m. on June 30, 2025, an executive at BMP Money Plus—a financial technology company specializing in banking-as-a-service (BaaS) solutions—was surprised by a phone call from CorpX Bank.



UNAUTHORIZED  
TRANSFER  
R\$ 18.000.000



CorpX Bank was warning about an unauthorized transfer of 18 million reais from BMP's reserve account.

The executive responsible for managing these reserves at the Central Bank quickly identified other, equally unauthorized transactions through PIX that were taking place at the same time.

**Unauthorized PIX  
Transactions**



**5:00 AM**

**C&M Software  
Incident Report**



The BMP team immediately began efforts to contain the situation, and at around 5 o'clock formally reported the incident to C&M Software, the company that provides them with critical payment processing services.

# Incident Timeline

🕒 **30/06/2025, 00h18**

Exchanges such as SmartPay and Truther detect large volumes and atypical transactions in Bitcoin/USDT, triggering FI executives.

🕒 **30/06/2025, 04h00**

BMP Money Plus Executive is informed about an extraordinary PIX of R\$ 18 million; several unauthorized transactions are identified.

🕒 **30/06/2025, 05h00**

Case reported to C&M Software by BMP executives.

🕒 **30/06/2025**

Central Bank orders emergency disconnection of C&M from SPB.

🕒 **01/07/2025**

Brazil Journal publishes detailed account of the attack.

🕒 **02/07/2025**

BMP Money Plus releases official statement confirming the incident.

🕒 **03/07/2025**

Central Bank Announces Partial Resumption of C&M Software Operations and Announces Arrest of Involved Employee

🕒 **04/07/2025**

Confirmed arrest of employee suspected of criminal collaboration

# Technical analysis of the incident

## Internal moderator



- PSTI employee co-opted by cybercriminals.
- Provided privileged access and executed malicious commands.

## Access and Scale



- Privileged access allowed them to map and obtain digital certificates from client FIs.
- They assumed the identities of the FIs without triggering alerts.

## Common structural failure



- Environments with centralized secrets without clear separation between client and PSTI increase the risk.
- Such attacks become more likely and more dangerous.

# Silent Injection: Fraudulent Orders at the Heart of the SPI

Attacks occurred outside of business hours, taking advantage of low human supervision.



## Step 1 Possession of Certificates



The FI's legitimate digital certificates were compromised



## Step 2 Injection of PIX Orders



Cybercriminals inject signed orders into SPI/SPB as if they were the FI's themselves



## Step 3 Automatic settlement



Transactions are settled automatically, without alerts - SPI assumes authenticity



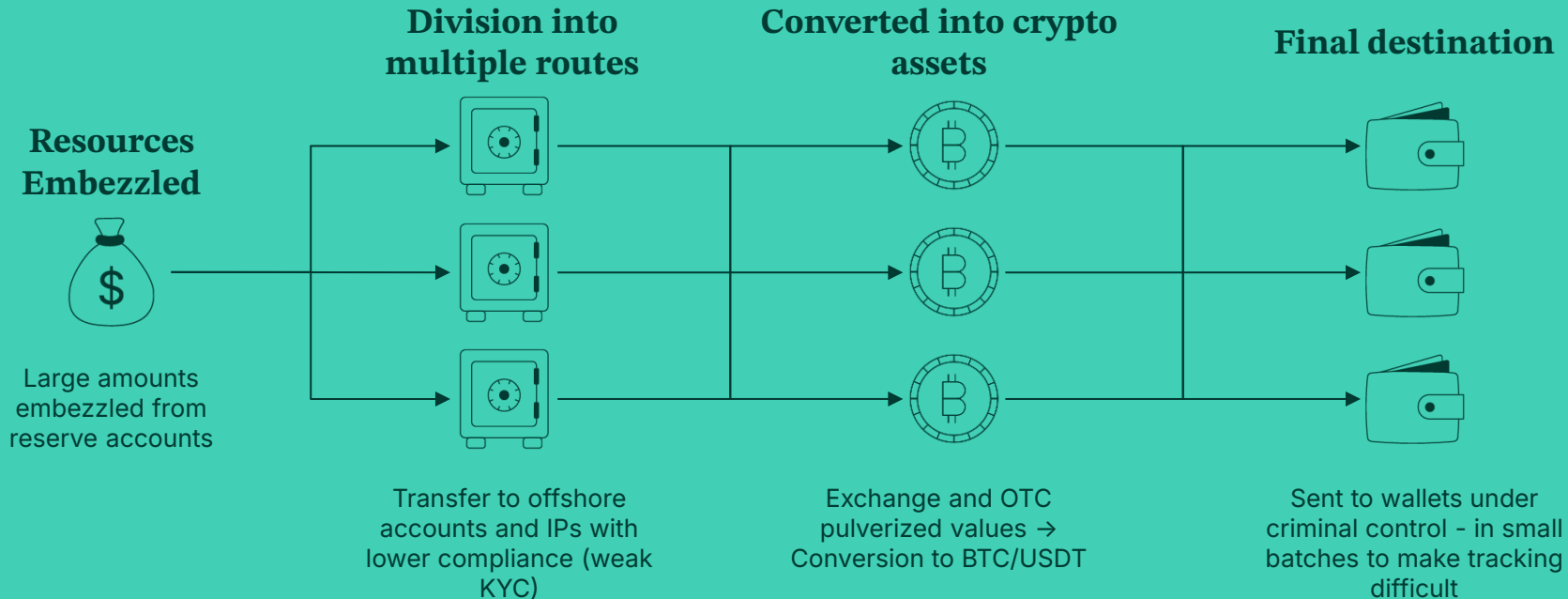
## Step 4 Debit the Reserve Accounts



Amounts are debited en masse from FI's accounts with the Central Bank

# Chain Dispersal: How the Attackers Laundered the Funds

Fragmentation, multiple routes, and anonymity make recovery extremely difficult.





# What about your organization?

Who has privileged access today?



Questions to Ask  
Yourself

1

Do you know exactly  
who has root access?

2

Are your sessions  
audited and  
monitored?

3








Do you have  
mandatory MFA and  
just-in-time access?

4

Do your certificates  
have a controlled  
lifecycle and  
automatic  
revocation?

# Could this have been avoided?

Yes, with governance and visibility.

 <b>Behavior Analytics</b>	Real-time detection of anomalous privileged access; automatic blocking in the event of deviations and correlation by geolocation, time, etc.
 <b>Just-in-Time Access</b>	Granting privileged access only for specific periods and tasks, reducing the risk window for insiders.
 <b>Credential rotation (based on anomalous behavior)</b>	Credentials automatically renewed in the event of any anomaly.
 <b>Secrets/Tokens Management for APIs and Supply Chain</b>	Vault tools for a secure and segregated cycle of third-party integrations and secrets.
 <b>Certificate Management and Rotation</b>	Automated monitoring and rotation of digital certificates used in critical operations.
 <b>Third-party access control</b>	Zero Trust policies for partners, rigorous onboarding/offboarding.
 <b>Reference Architecture</b>	Visual proposal for integrated security design for PSTIs, FIs and Bacen (flowchart or diagram).

# How Segura<sup>®</sup> works on all fronts

Segura<sup>®</sup> solutions for every vulnerable link in the chain



## PAM Core

**Privileged Access Management Including**

- Behavior Analytics
- Just-in-Time Access
- Credential rotation

And much more...



## Certificate Manager

**Certificate lifecycle management Including**

- Automatic rotation
- Certificate usage monitoring

And much more...



## Domum

**Remote access management without VPN Including**

- Third-party access management
- Session recording
- Just-in-Time access

And much more...



## DevOps Secret Manager

**DevOps secrets management Including**

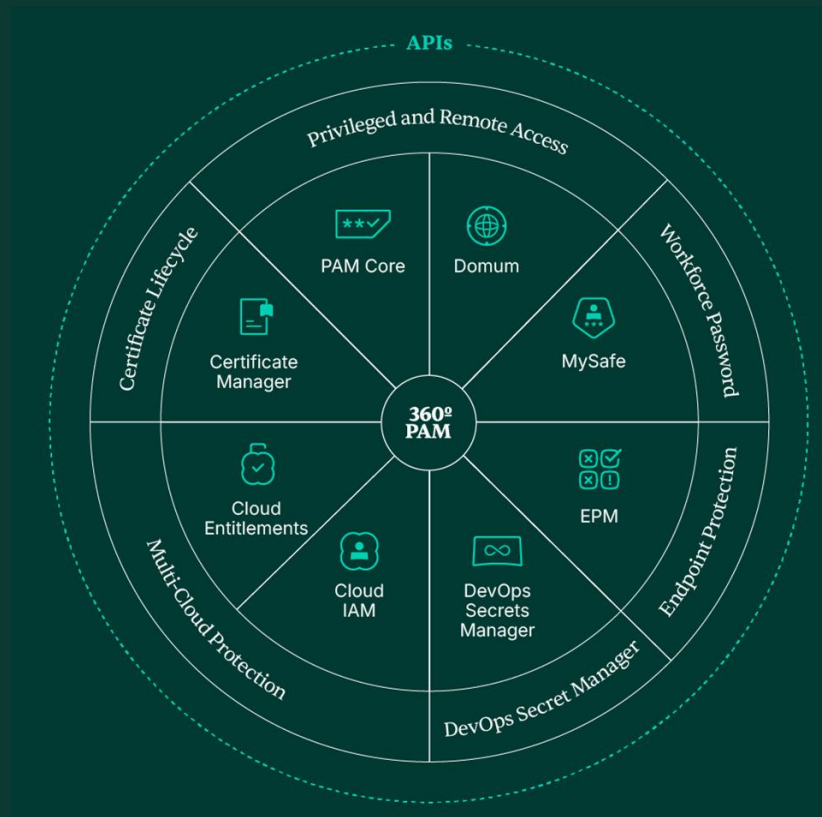
- Third-party access management
- Session recording
- Just-in-Time access

And much more...

# 360° Privilege Platform

Fast. Simple. Secure.

Everything you need to control  
privileged accesses.





# Segura<sup>®</sup> Platform Products

	<b>PAM Core</b>	Protects, controls and audits privileged access and critical credentials.
	<b>Domum Remote Access</b>	Allows secure remote access without VPN, with full session auditing and monitoring.
	<b>DevOps Secret Manager (DSM)</b>	Manages and protects secrets and credentials in DevOps pipelines.
	<b>Certificate Manager (CLM)</b>	Automates the complete lifecycle of digital certificates (issuance, renewal, etc.).
	<b>Endpoint Privilege Manager (EPM)</b>	Enforces least privilege on workstations and servers (Windows, Linux, macOS).
	<b>MySafe</b>	Enterprise password vault for secure storage, generation, and automatic filling of credentials.
	<b>Cloud Entitlements (CIEM)</b>	Ensures visibility and control over identities and permissions in cloud providers (AWS, Azure, GCP, Oracle).

# Why choose Segura®



## Agentless Architecture

No third-party services  
or complex integrations.



## Fast Deployment

In hours, not weeks.



## Native Governance

100% aligned with  
Compliance and policies.



## One Platform Experience

Natively integrates access  
management solutions,  
certificates, secrets,  
credentials and more.



## Best rated by real users

**4.9/5 on**  
Gartner Peer Insights.



## Lower TCO

More value, less cost - the  
lowest TCO on the market.

# Let's assess your risk exposure?

Schedule a free session with our experts to identify the main points of attention in your access and certificate governance.

