Security and Privacy assessment of UPI protocol in PhonePe

Super honorable professor
Jan Tobias Mühlberg

Arun Poovelikunnel Varghese
Zakaria Belkadi

Objective

01 Introduction

02 Data Flow Diagram

03 Threat Modelling with LINDDUN GO and STRIDE

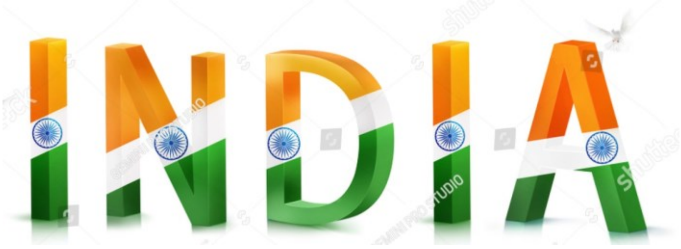
04 CONCLUSION

Joke

What's better than a mobile payment app ?

Joke

What's better than a mobile payment app ?

A mobile payment app from 

Introduction

PhonePe

PhonePe is mobile payment platform of India

Offers diverse services instant money transfer, bill payment, and integration with various merchants.

Operates on Unified Payment Interface that enable instant, secure and interoperable transaction between banks.

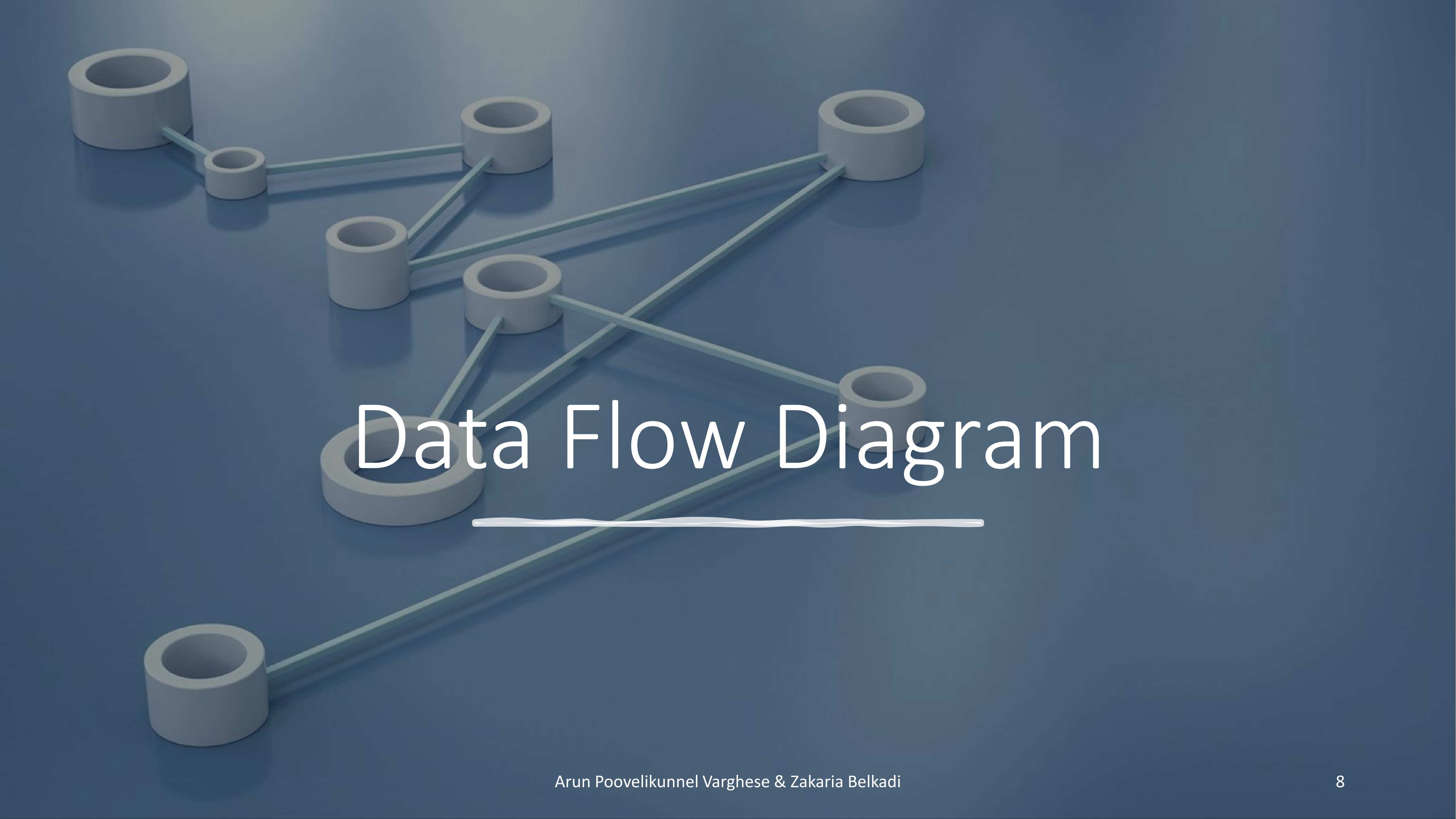
Acts as a centralized platform to link different bank accounts.

Unified Payment Interface

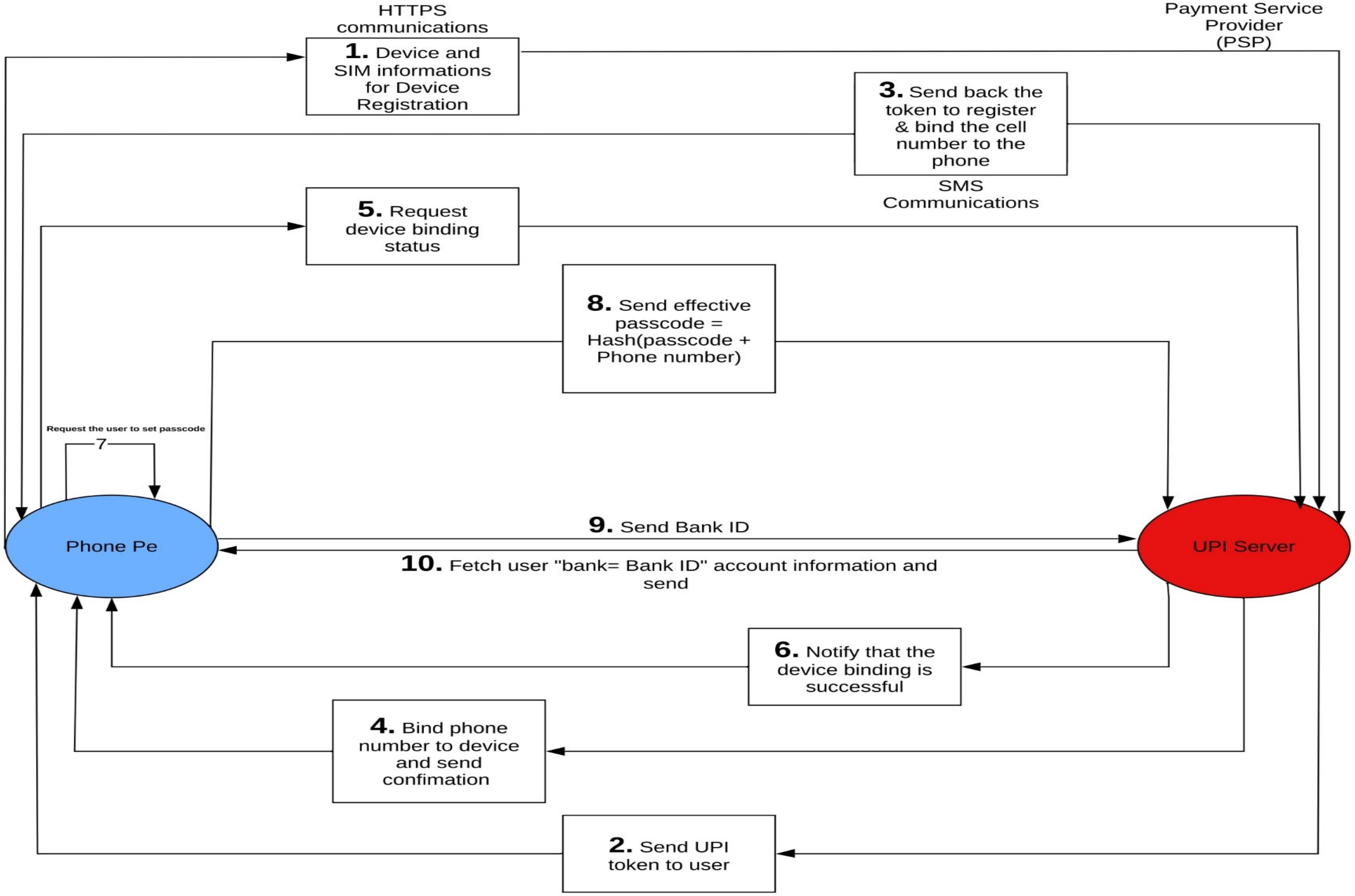
UPI is a Digital India initiative.

UPI is standardized framework developed by National Payments Corporation of India (NPCI) to facilitate real-time payments between banks and framework launched in 2016 August.

Uses Virtual Payment Address (VPA) for transaction.



Data Flow Diagram


HTTPS communications
1. Device and SIM informations for Device Registration
Payment Service Provider (PSP)
3. Send back the token to register & bind the cell number to the phone
SMS Communications
5. Request device binding status
8. Send effective passcode = Hash(passcode + Phone number)
Request the user to set passcode
7
Phone Pe
9. Send Bank ID
UPI Server
10. Fetch user "bank= Bank ID" account information and send
6. Notify that the device binding is successful
4. Bind phone number to device and send confimation
2. Send UPI token to user

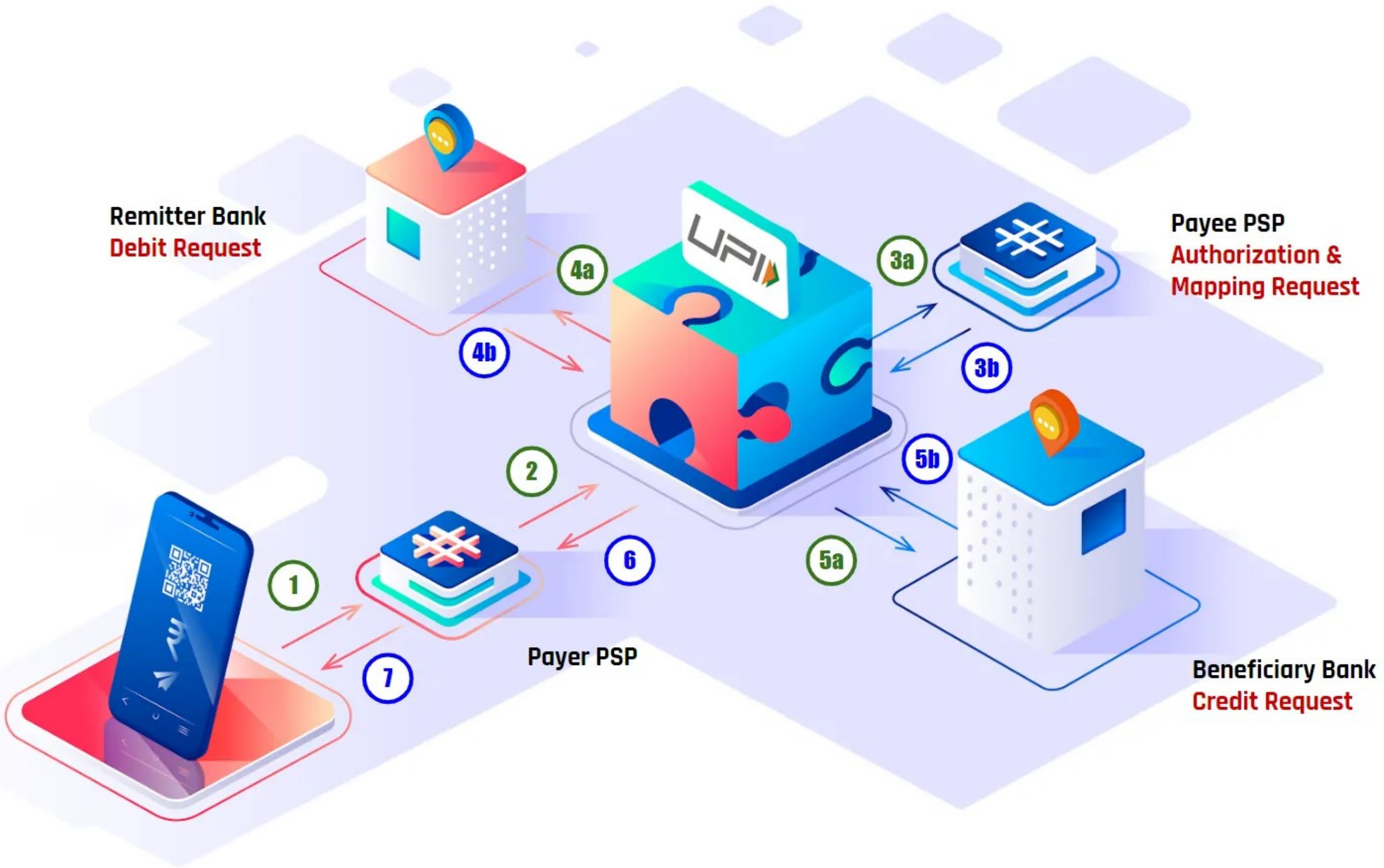
Post registration

After completing the registration the user will :

Get a unique UPI ID across all UPI system

Get a QR code to Receive money

UPI Transaction Flow



Remitter Bank
Debit Request

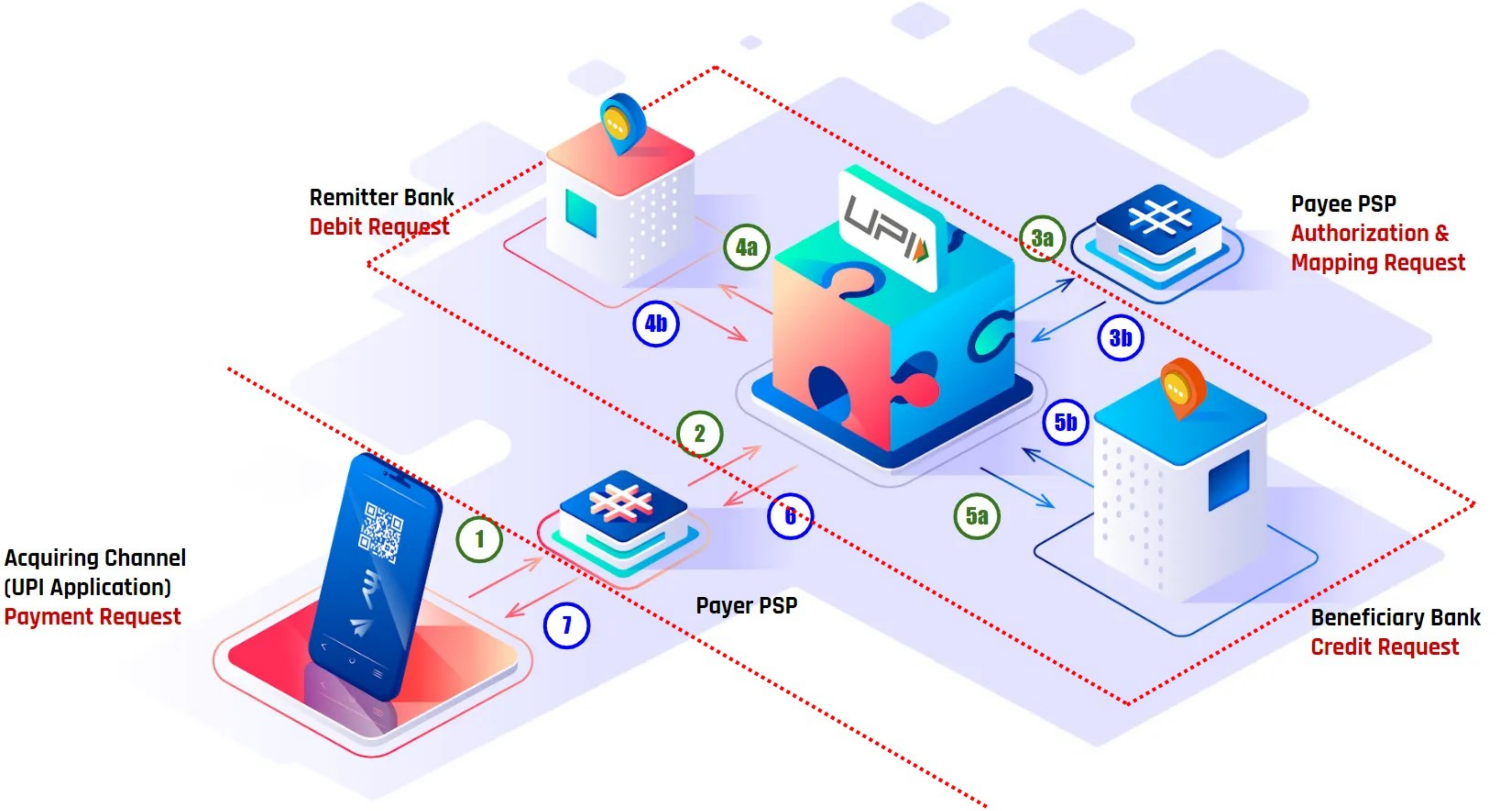
Payee PSP
Authorization &
Mapping Request

Acquiring Channel
(UPI Application)
Payment Request

Payer PSP

Beneficiary Bank
Credit Request

UPI Transaction Flow



Remitter Bank
Debit Request

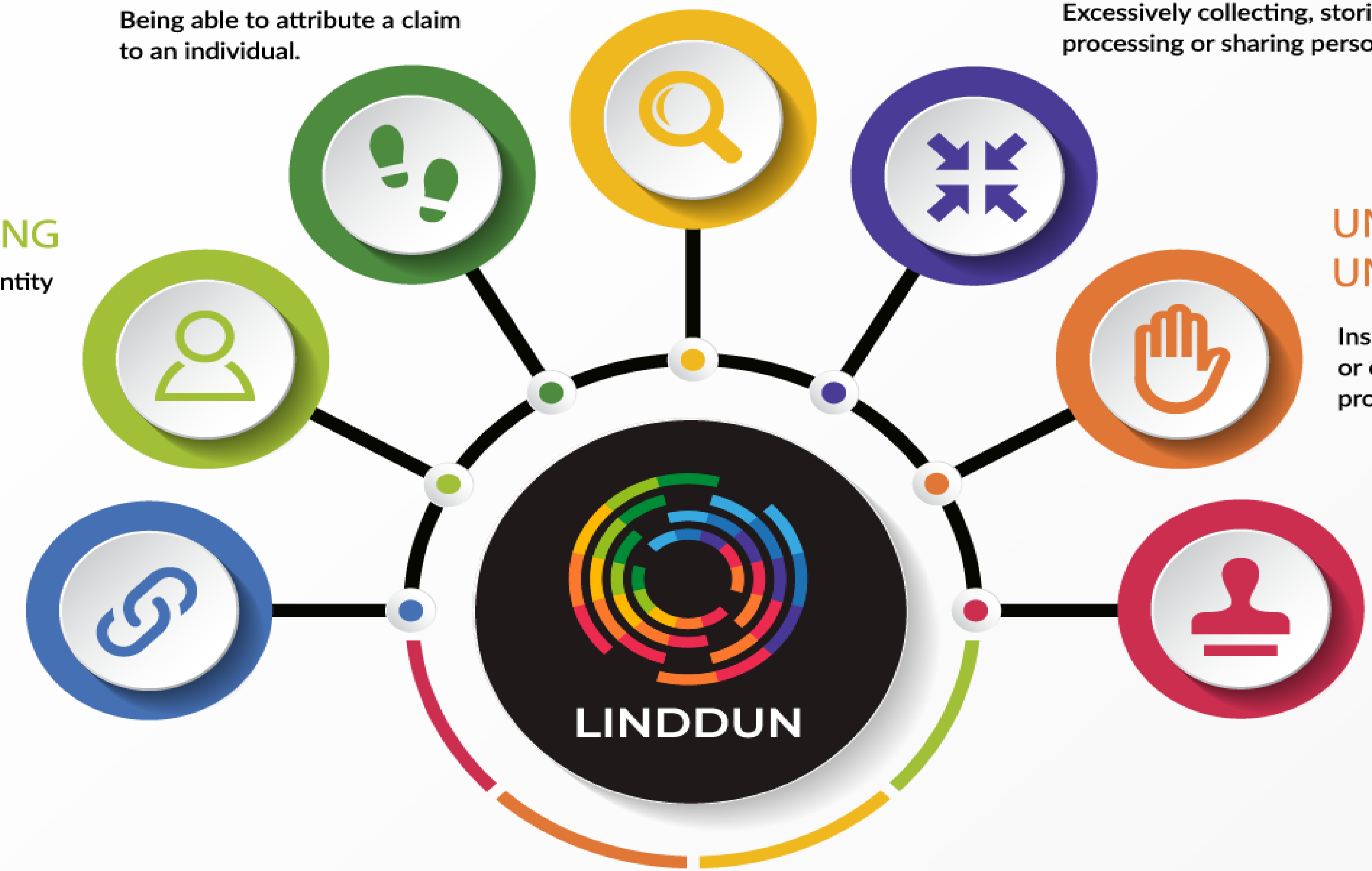
Payee PSP
Authorization & Mapping Request

Acquiring Channel
(UPI Application)
Payment Request

Payer PSP

Beneficiary Bank
Credit Request

Threat Modelling



LINKING

Associating data items or user actions to learn more about an individual or group.

IDENTIFYING

Learning the identity of an individual.

NON-REPUDIATION

Being able to attribute a claim to an individual.

DETECTING

Deducing the involvement of an individual through observation.

DATA DISCLOSURE

Excessively collecting, storing, processing or sharing personal data.

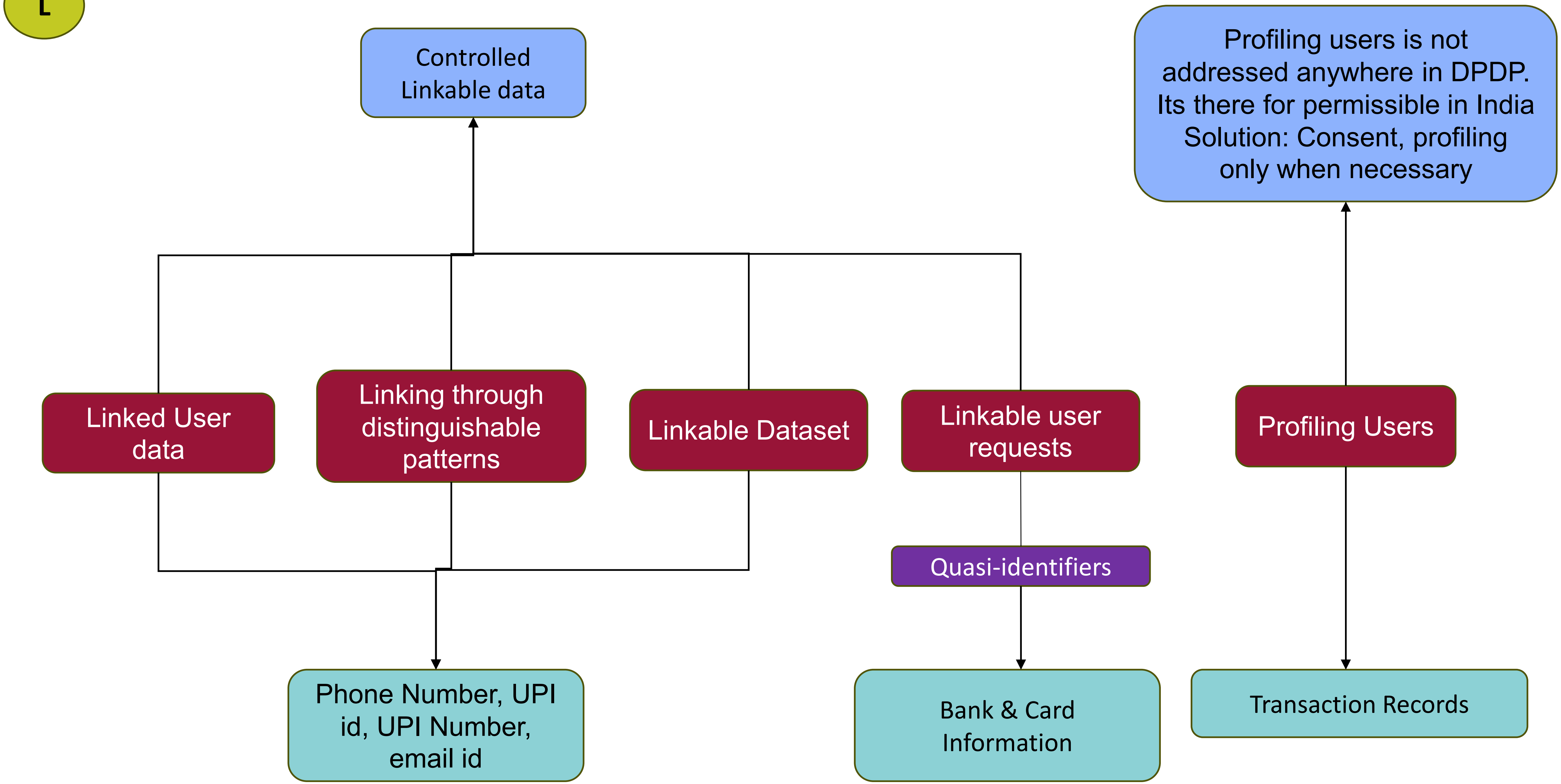
UNAWARENESS & UNINTERVENABILITY

Insufficiently informing, involving or empowering individuals in the processing of personal data.

NON-COMPLIANCE

Deviating from security and data management best practices, standards and legislation.

L



Controlled Linkable data

Profiling users is not addressed anywhere in DPDP. Its there for permissible in India Solution: Consent, profiling only when necessary

Linked User data

Linking through distinguishable patterns

Linkable Dataset

Linkable user requests

Profiling Users

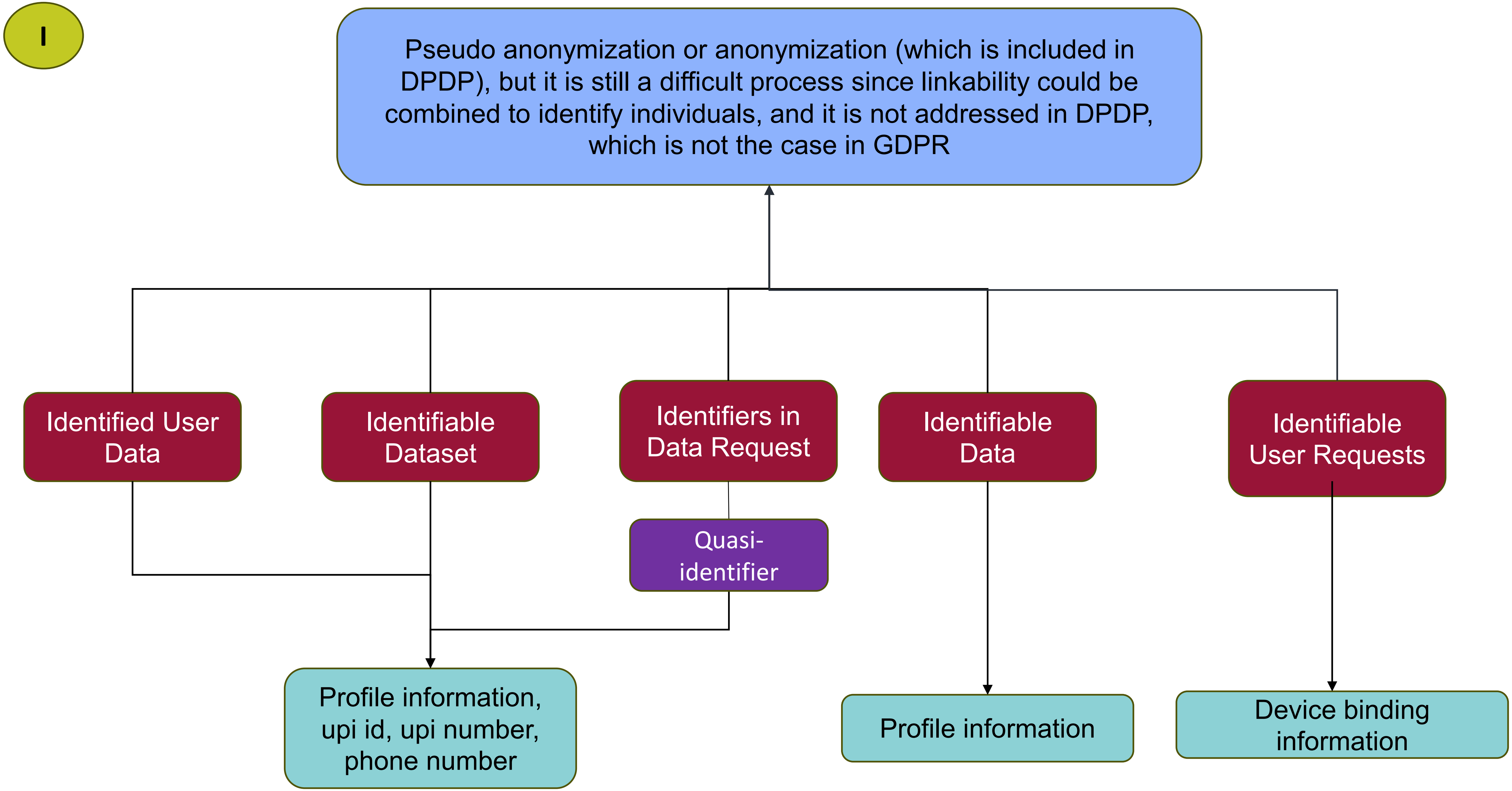
Quasi-identifiers

Phone Number, UPI id, UPI Number, email id

Bank & Card Information

Transaction Records

I



Pseudo anonymization or anonymization (which is included in DPDP), but it is still a difficult process since linkability could be combined to identify individuals, and it is not addressed in DPDP, which is not the case in GDPR

Identified User Data

Identifiable Dataset

Identifiers in Data Request

Identifiable Data

Identifiable User Requests

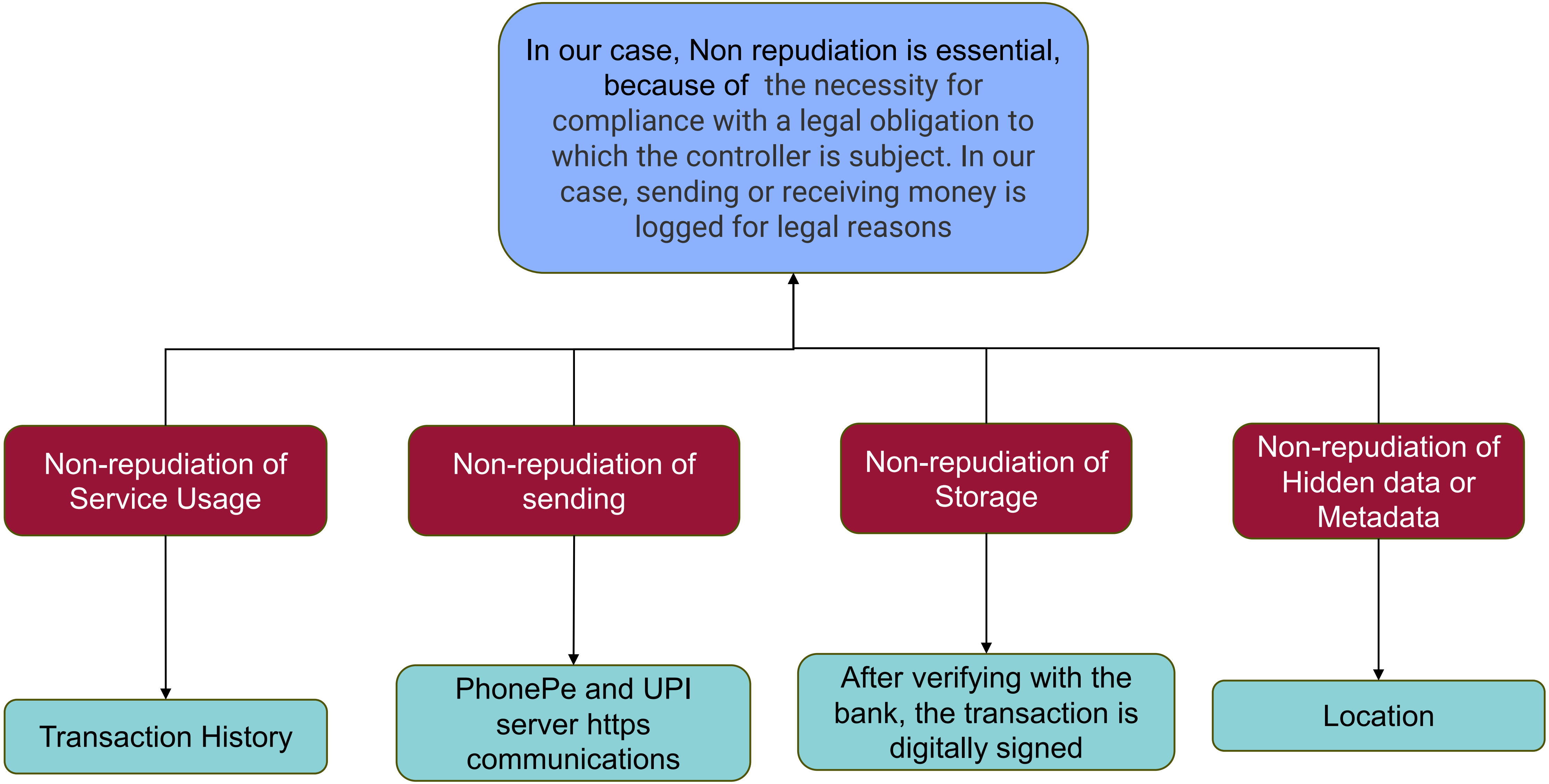
Quasi-identifier

Profile information, upi id, upi number, phone number

Profile information

Device binding information

N



In our case, Non repudiation is essential, because of the necessity for compliance with a legal obligation to which the controller is subject. In our case, sending or receiving money is logged for legal reasons

Non-repudiation of Service Usage

Transaction History

Non-repudiation of sending

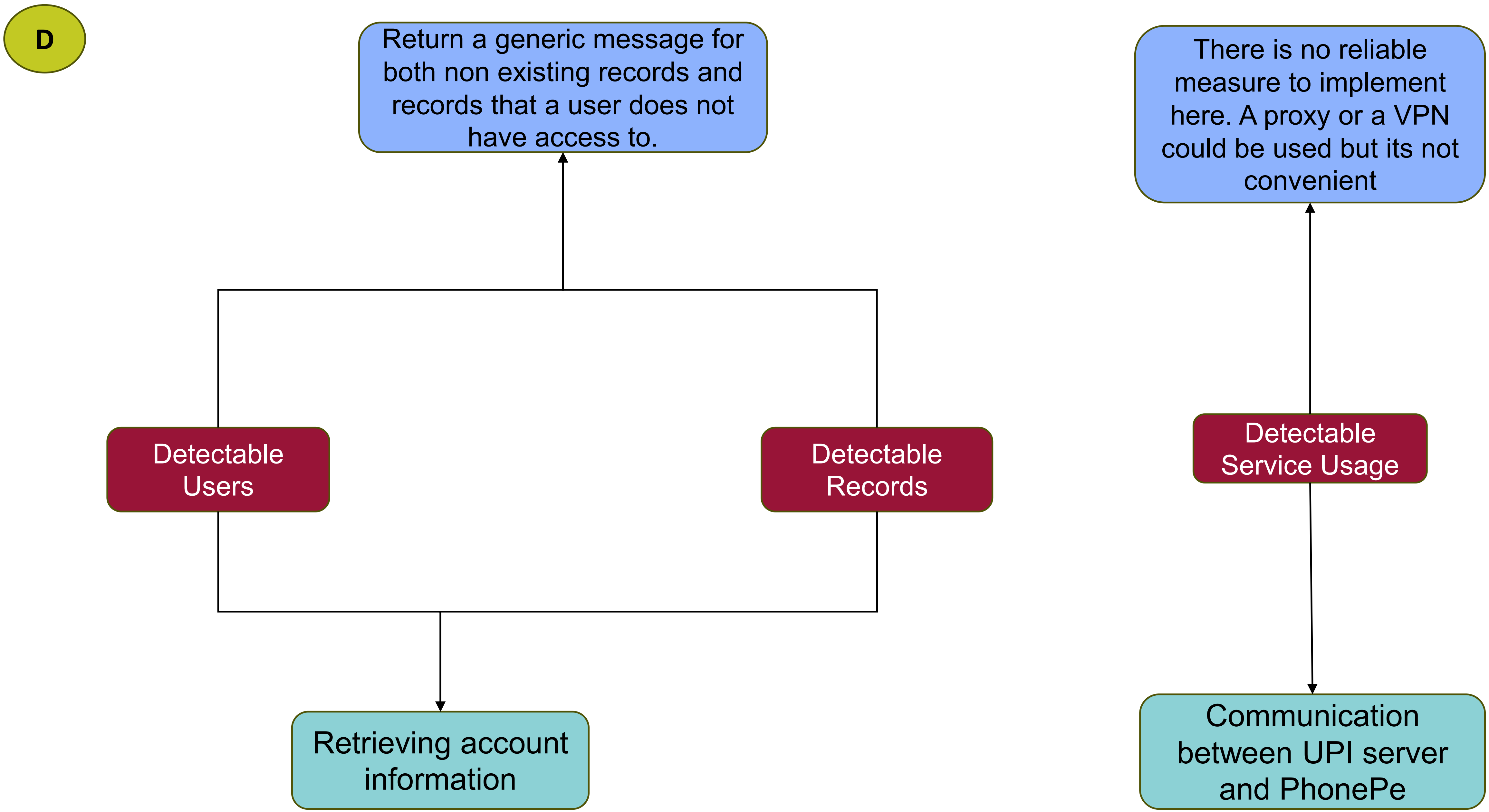
PhonePe and UPI server https communications

Non-repudiation of Storage

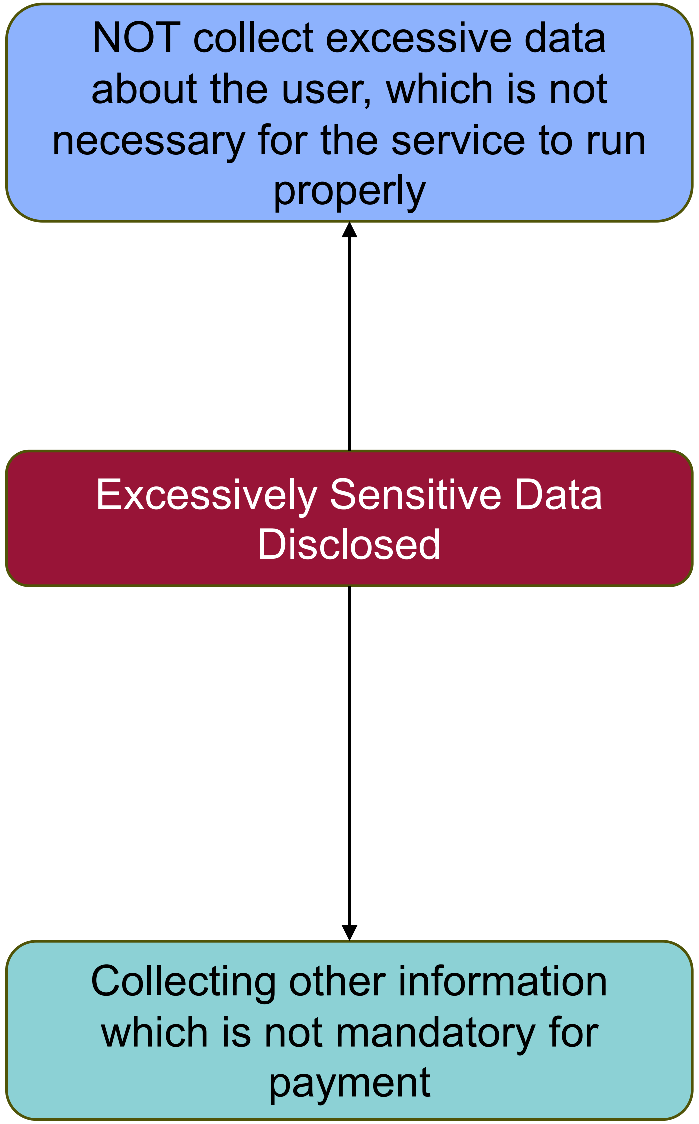
After verifying with the bank, the transaction is digitally signed

Non-repudiation of Hidden data or Metadata

Location


D
Return a generic message for both non existing records and records that a user does not have access to.
There is no reliable measure to implement here. A proxy or a VPN could be used but its not convenient
Detectable Users
Detectable Records
Detectable Service Usage
Retrieving account information
Communication between UPI server and PhonePe

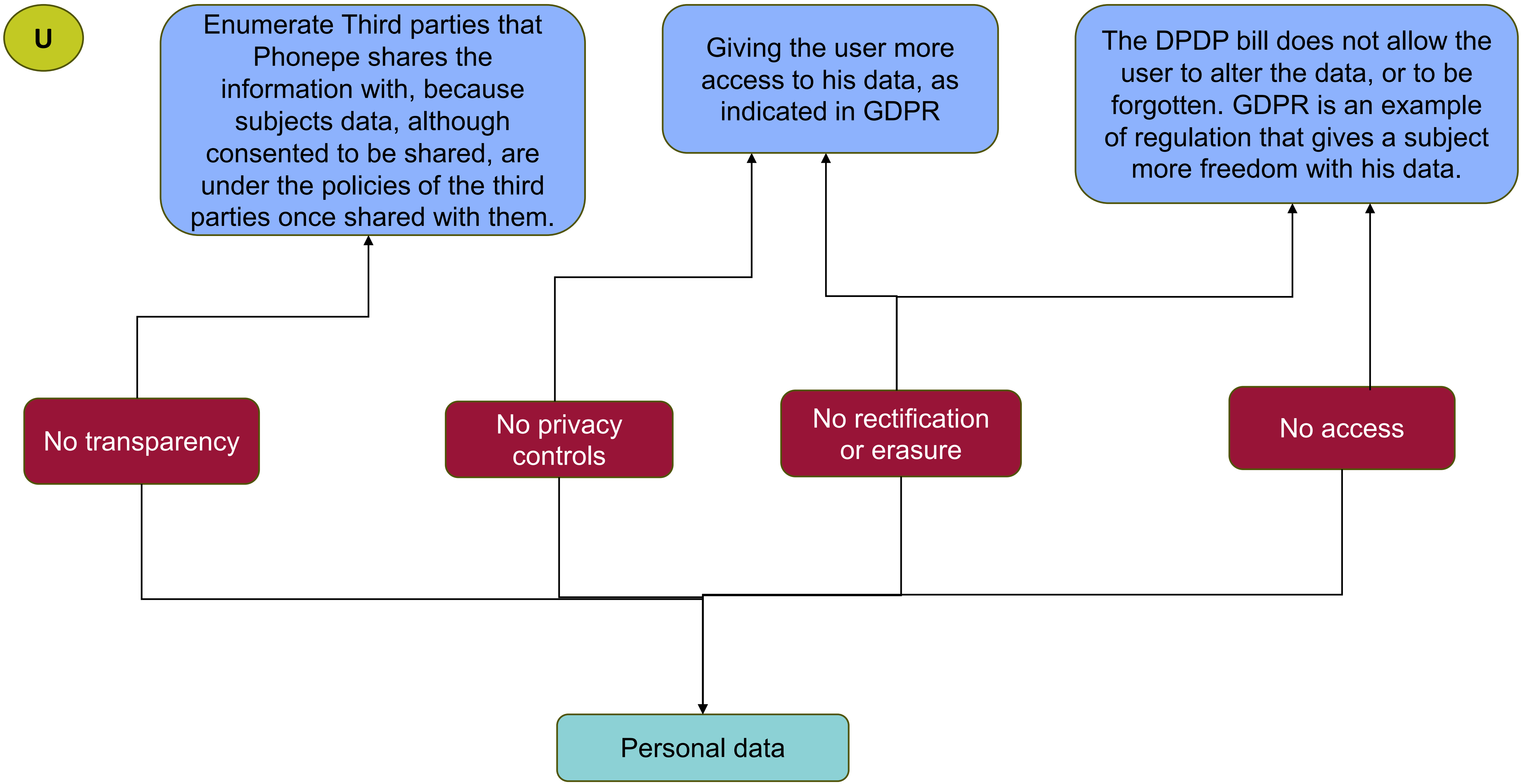
D



NOT collect excessive data about the user, which is not necessary for the service to run properly

Excessively Sensitive Data Disclosed

Collecting other information which is not mandatory for payment



U

Enumerate Third parties that Phonepe shares the information with, because subjects data, although consented to be shared, are under the policies of the third parties once shared with them.

Giving the user more access to his data, as indicated in GDPR

The DPDP bill does not allow the user to alter the data, or to be forgotten. GDPR is an example of regulation that gives a subject more freedom with his data.

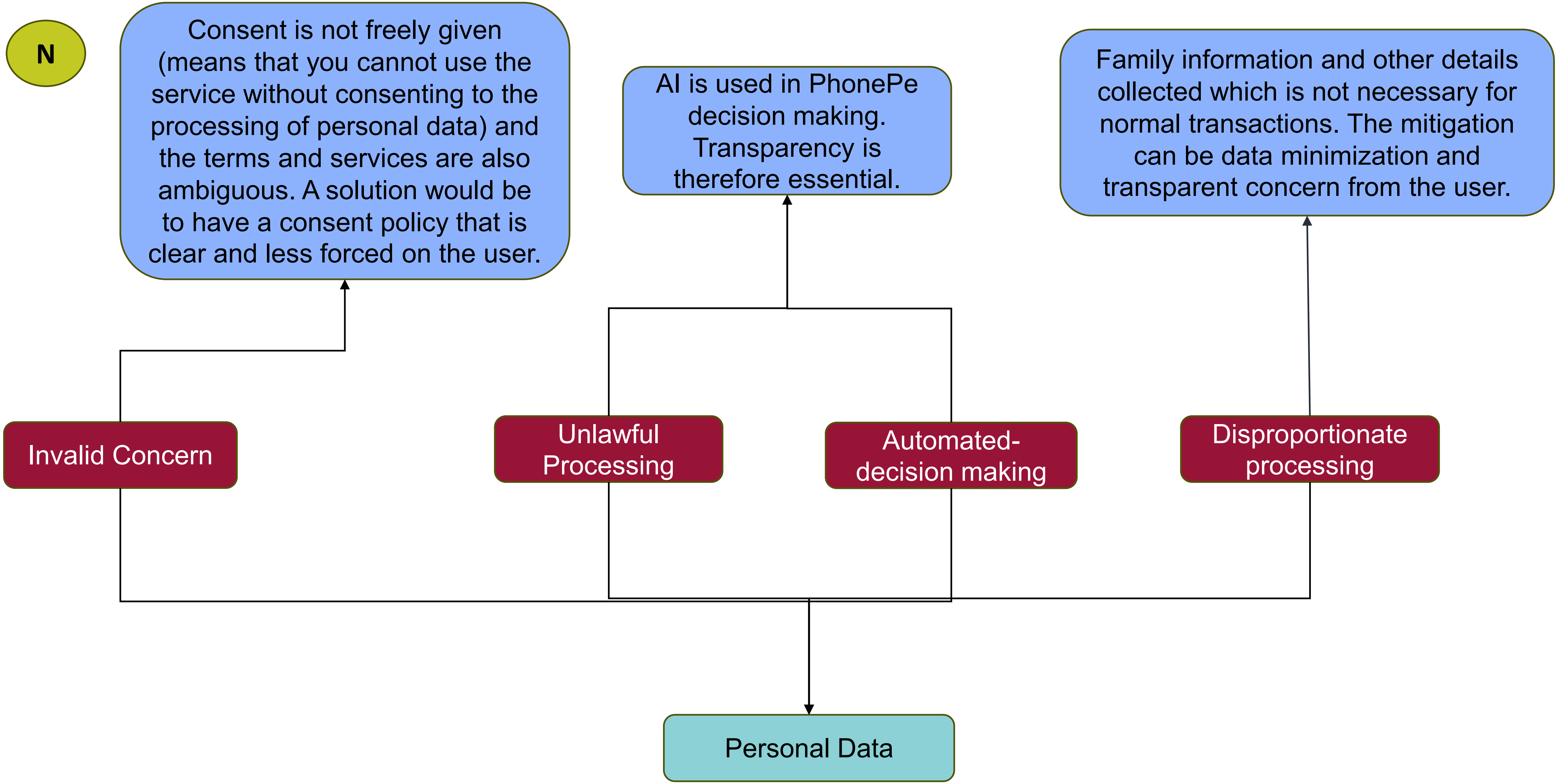
No transparency

No privacy controls

No rectification or erasure

No access

Personal data

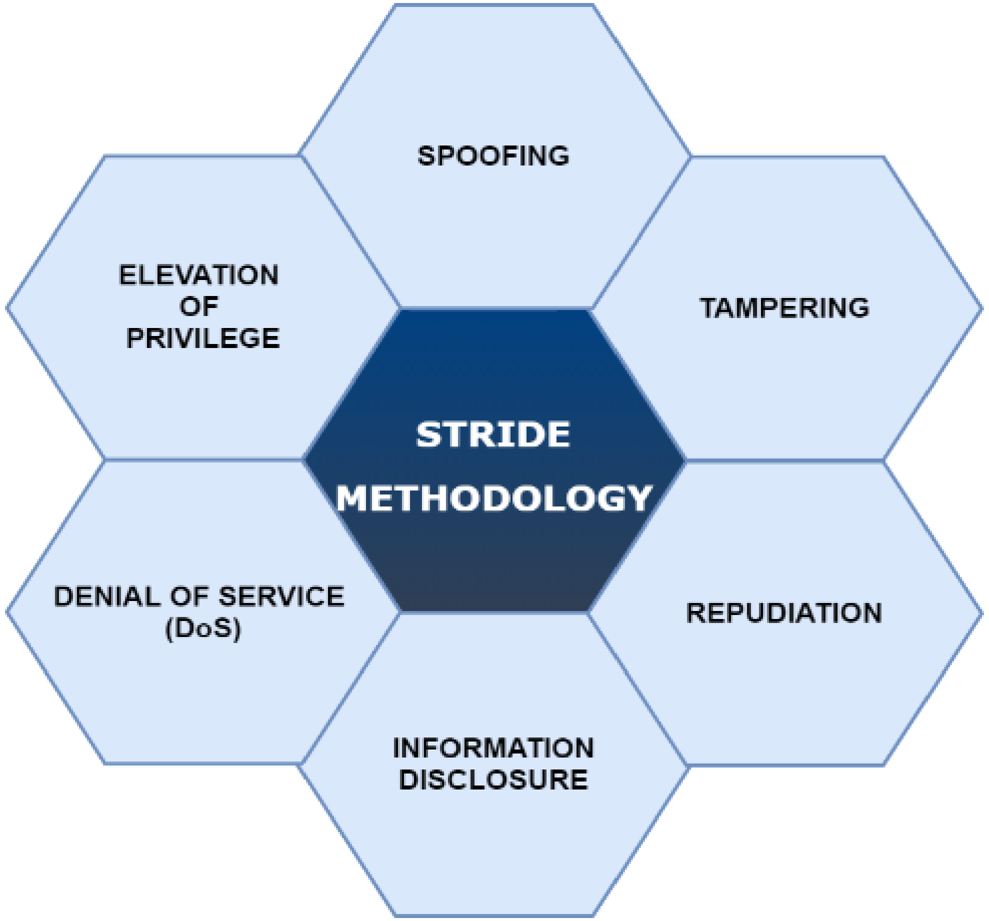


N

Consent is not freely given (means that you cannot use the service without consenting to the processing of personal data) and the terms and services are also ambiguous. A solution would be to have a consent policy that is clear and less forced on the user.

AI is used in PhonePe decision making. Transparency is therefore essential.

Family information and other details collected which is not necessary for normal transactions. The mitigation can be data minimization and transparent concern from the user.



STRIDE METHODOLOGY

SPOOFING

TAMPERING

REPUDIATION

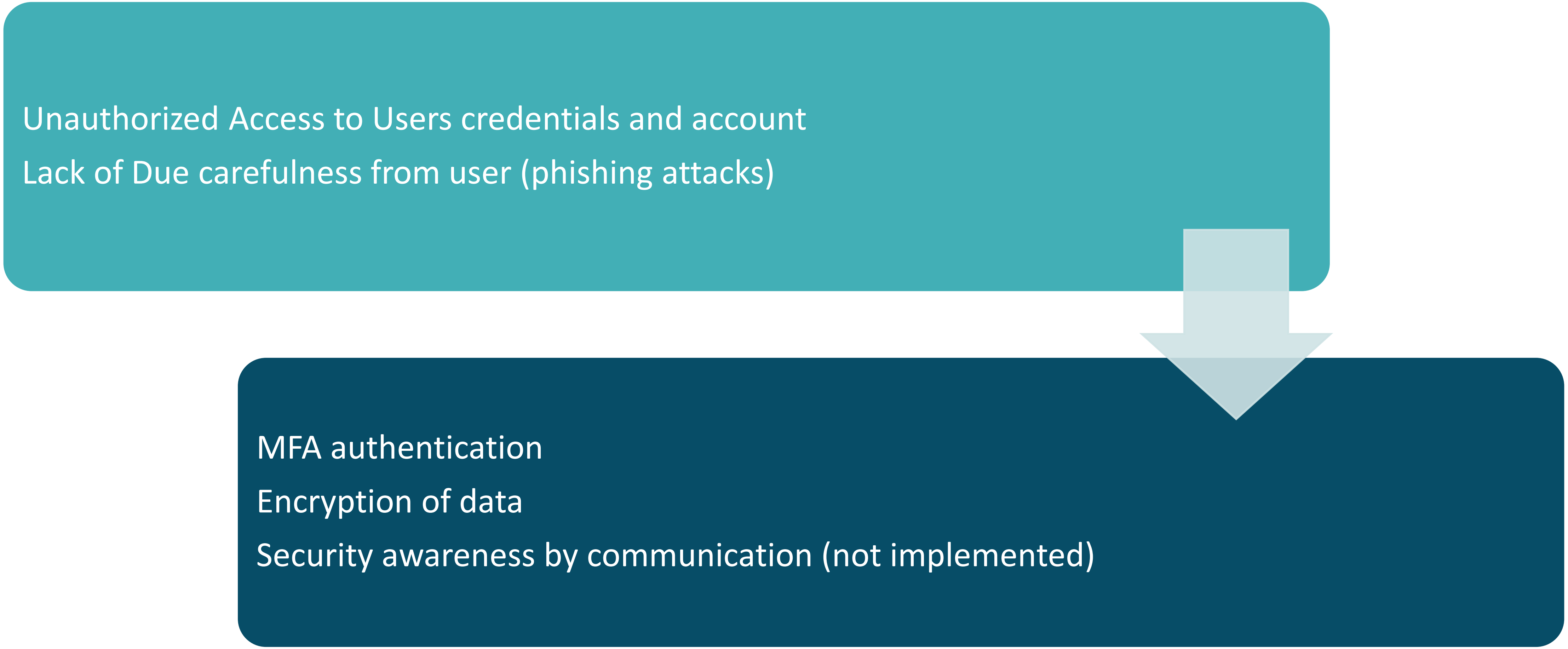
INFORMATION DISCLOSURE

DENIAL OF SERVICE (DoS)

ELEVATION OF PRIVILEGE

Assets	S	T	R	I	D	E
User Data	X	X		X		
Banking Data (Bank account details, UPI ID)						
Personal Data						
Mobile device		X		X		
PhonePe app (code,...)		X		X		X
Physical SIM	X	X		X		
Communication	X	X		X		
Third party integration (merchant, Acquirers, Providers)	X	X		X	X	
Transactions	X	X	X	X		
UPI server	X		X		X	X

User Information



Unauthorized Access to Users credentials and account

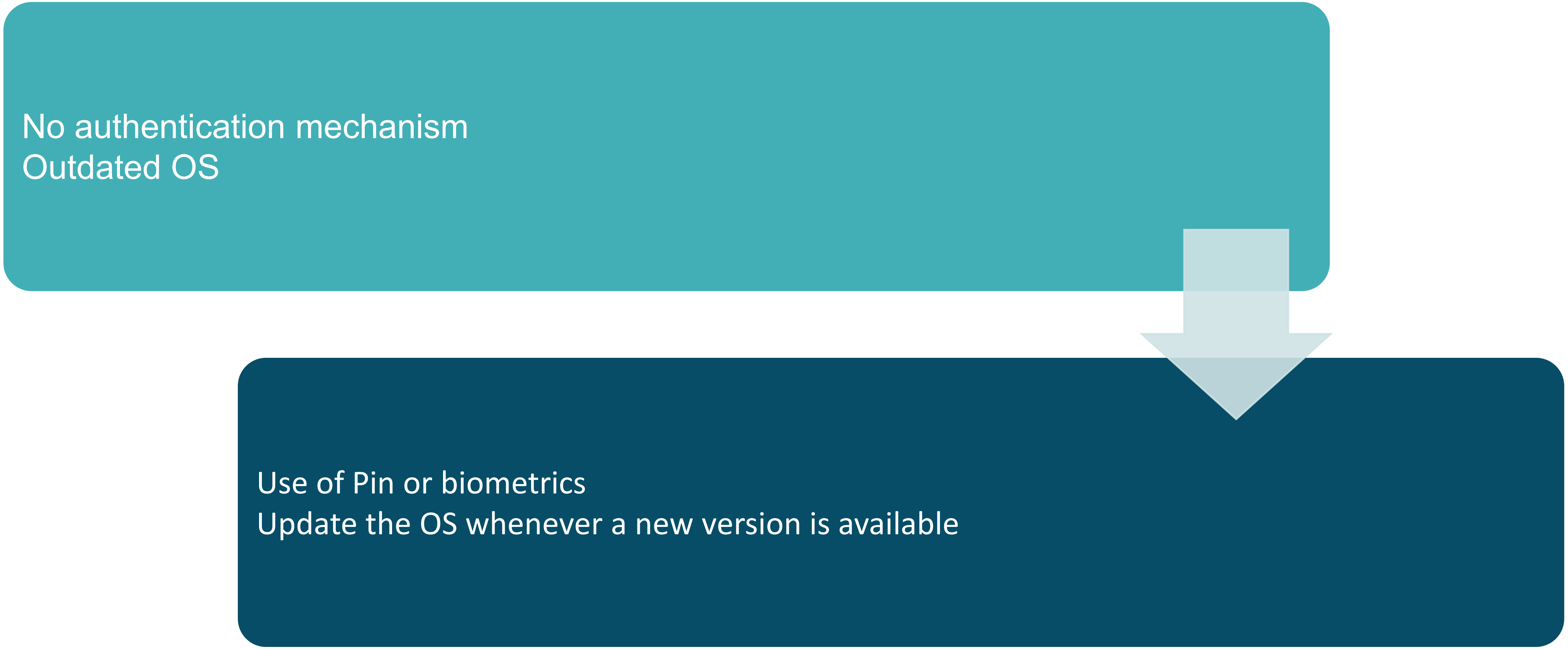
Lack of Due carefulness from user (phishing attacks)

MFA authentication

Encryption of data

Security awareness by communication (not implemented)

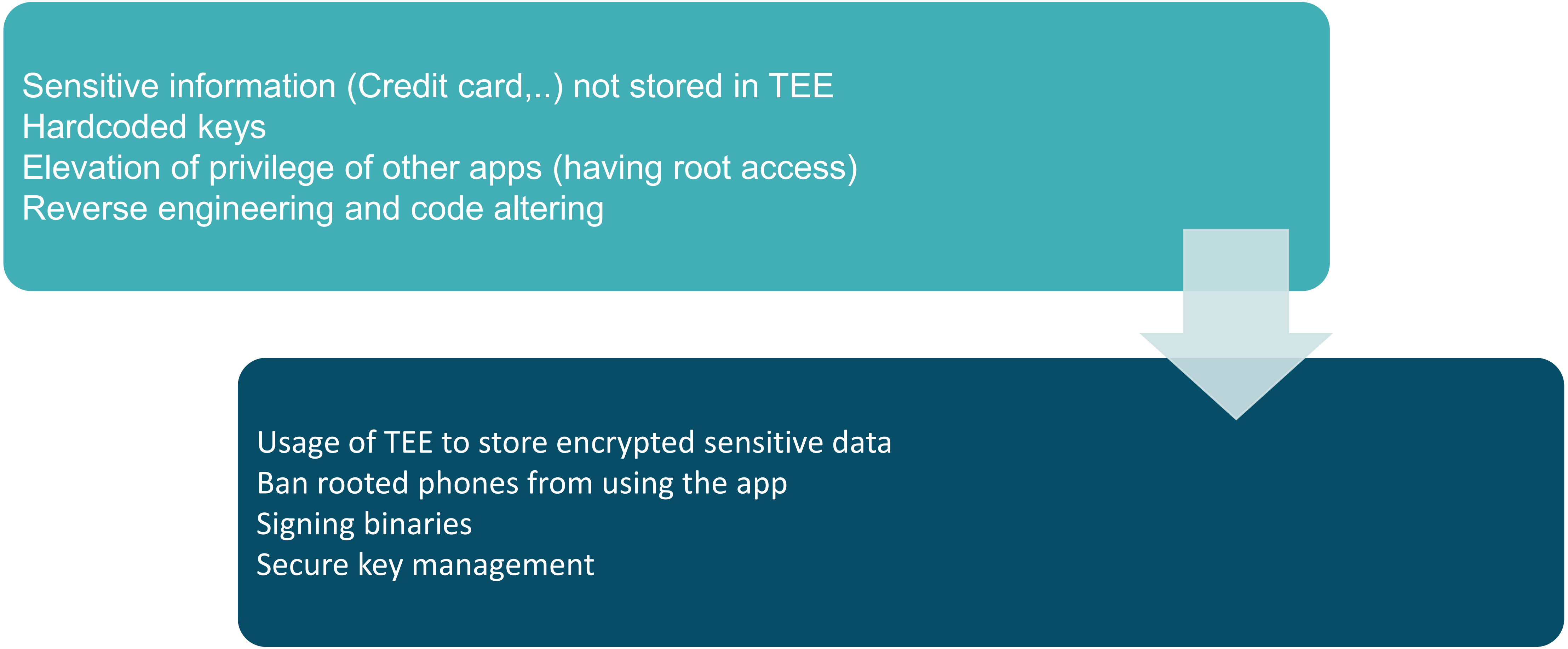
Mobile Device



No authentication mechanism
Outdated OS

Use of Pin or biometrics
Update the OS whenever a new version is available

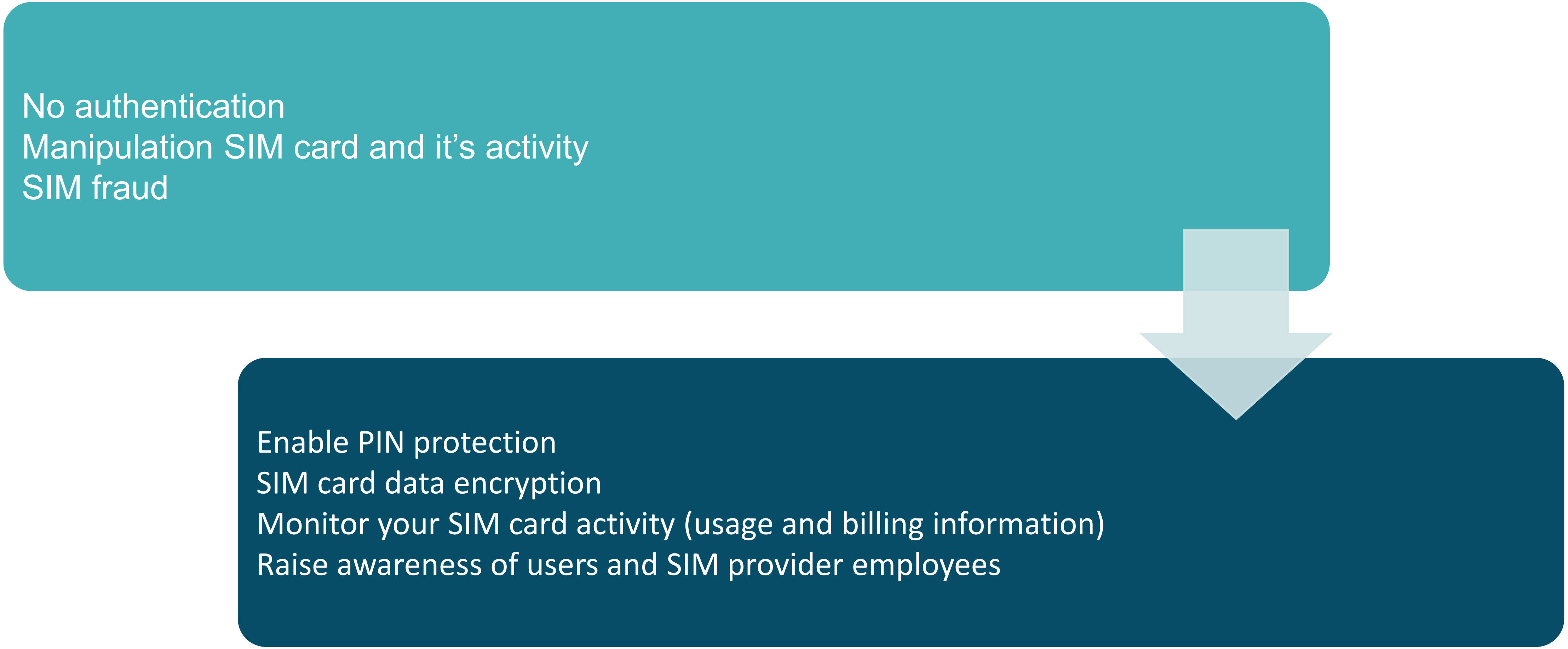
PhonePe app (code,...)



Sensitive information (Credit card,..) not stored in TEE
Hardcoded keys
Elevation of privilege of other apps (having root access)
Reverse engineering and code altering

Usage of TEE to store encrypted sensitive data
Ban rooted phones from using the app
Signing binaries
Secure key management

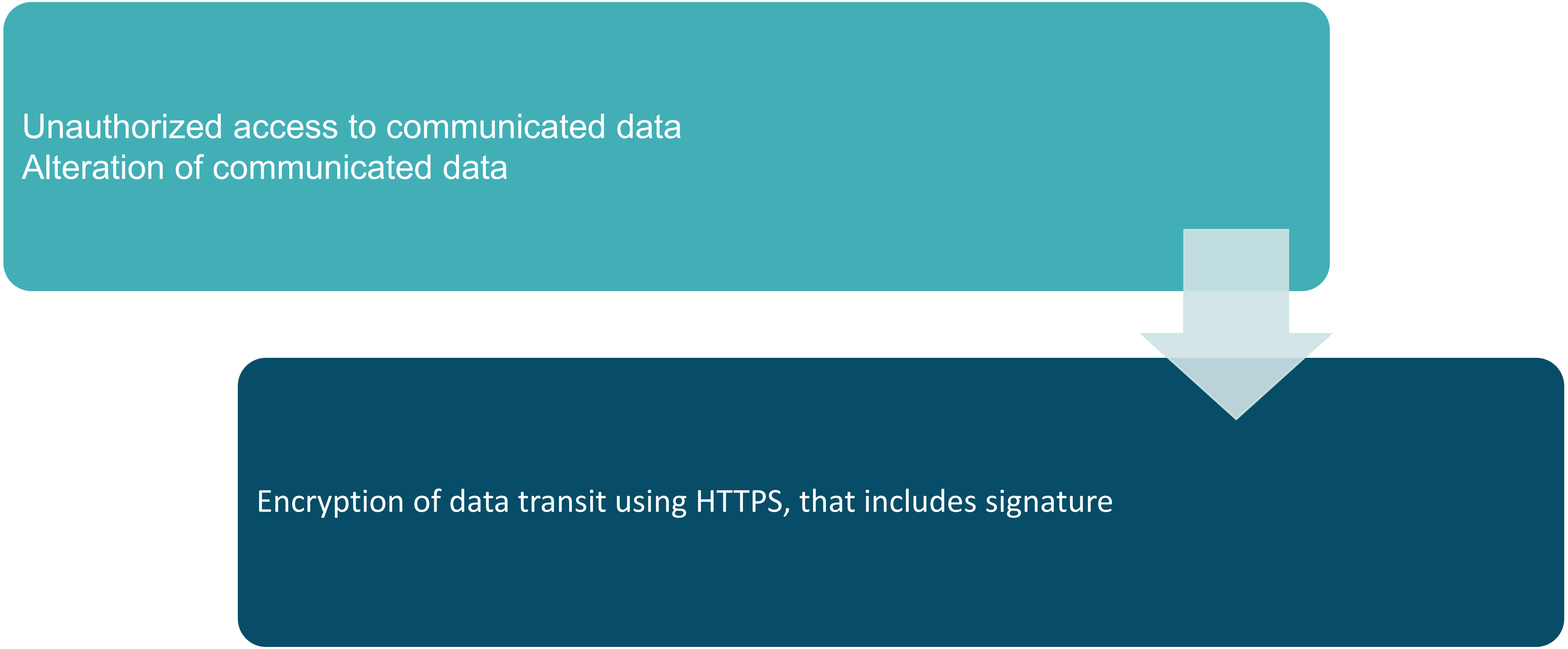
Physical SIM



No authentication
Manipulation SIM card and it’s activity
SIM fraud

Enable PIN protection
SIM card data encryption
Monitor your SIM card activity (usage and billing information)
Raise awareness of users and SIM provider employees

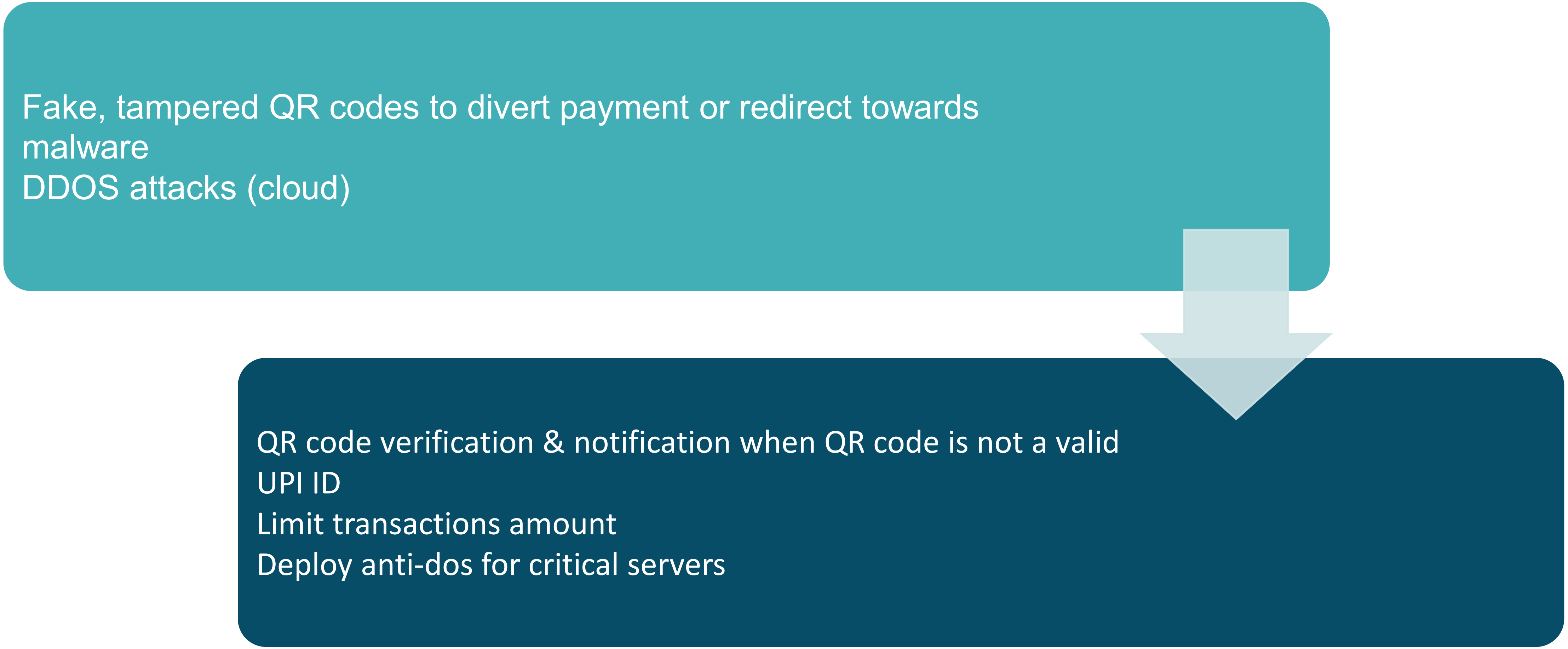
Communication



Unauthorized access to communicated data
Alteration of communicated data

Encryption of data transit using HTTPS, that includes signature

Third party integration



Fake, tampered QR codes to divert payment or redirect towards malware

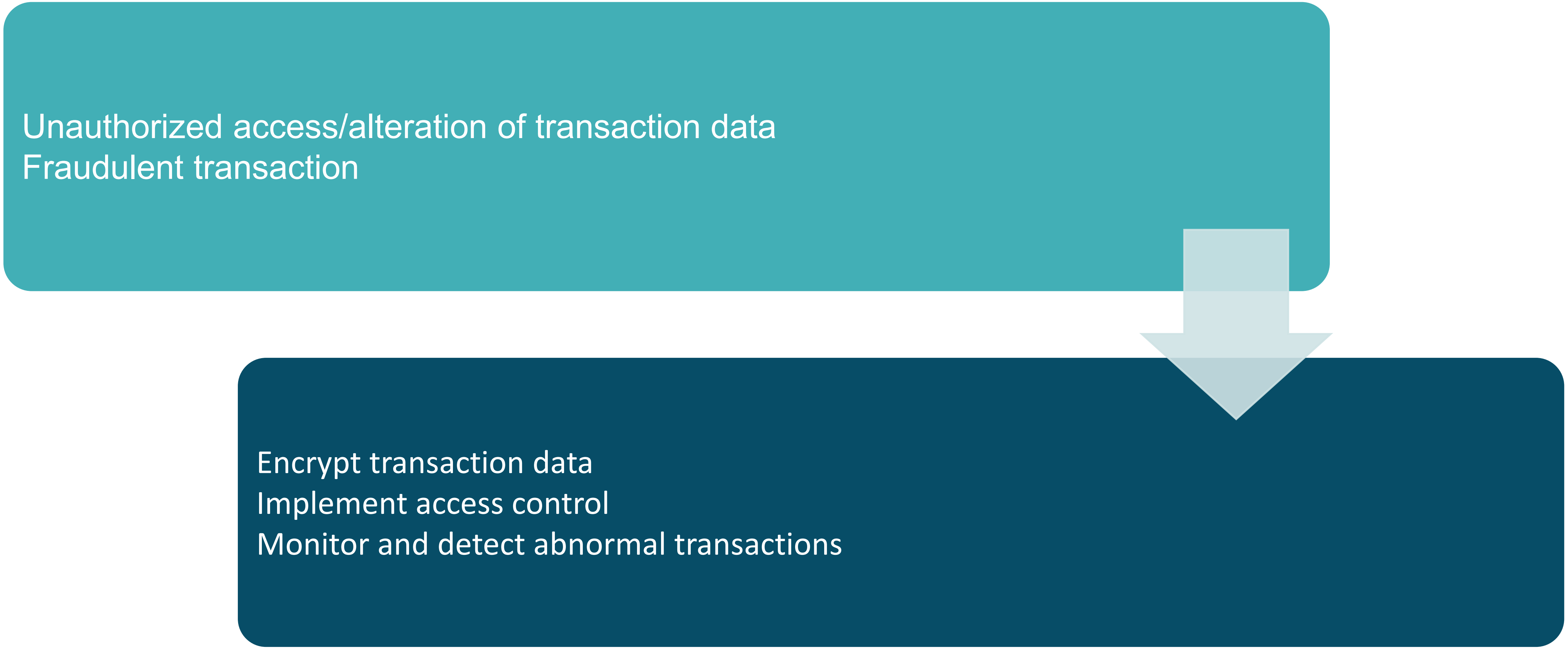
DDOS attacks (cloud)

QR code verification & notification when QR code is not a valid UPI ID

Limit transactions amount

Deploy anti-dos for critical servers

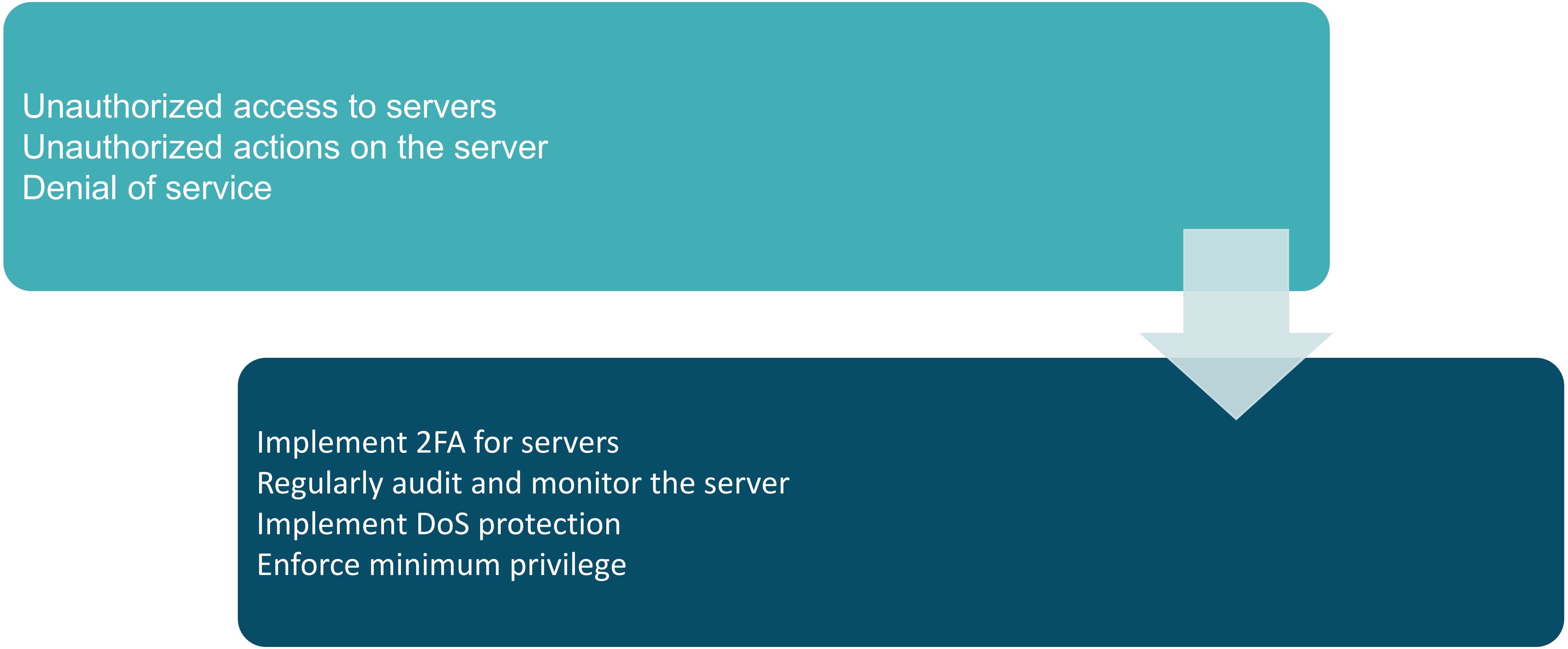
Transactions



Unauthorized access/alteration of transaction data
Fraudulent transaction

Encrypt transaction data
Implement access control
Monitor and detect abnormal transactions

UPI server



Unauthorized access to servers
Unauthorized actions on the server
Denial of service

Implement 2FA for servers
Regularly audit and monitor the server
Implement DoS protection
Enforce minimum privilege

MFA, encryption of data in transit,

QR code verification & notification when QR code is not a valid UPI ID

Usage of TEE to store encrypted sensitive data

Signing binaries, Secure key management and Enforce minimum privilege

Regularly audit and monitor the server, Implement DoS protection

Ban rooted phones from using the app,

Raise awareness of users and SIM provider employees

Security awareness by communication (not implemented)

Monitor and detect abnormal transactions

Enable PIN protection

SIM card data encryption

Monitor your SIM card activity (usage and billing information)

Update the OS whenever a new version is available

Limit transactions amount

Conclusion

- PhonePe (& UPI in general) is a convenient way to send/receive money
- But !... Convenience comes at a price
- Applying LINDDUN GO on PhonePe shows the differences between DPDP & GDPR
- STRIDE and LINDDUN are complementary, its not a matter of choosing one or the other

Reference

- Security Analysis of Unified Payments Interface and Payment Apps in India (Slide 9)
- LINDDUN GO (Slide 14)
- STRIDE (Slide 22)
- Detailed Data Flow Diagram (Slide 11, 12)

Thank you