

# City resident becomes a victim of identity theft

6 loans worth ₹4 lakh taken in his name by a fraudster from three different banks & 3 finance companies

ANURAG KUMAR

DELHI

The next time someone asks you to share details of your identity proof or its pictures on WhatsApp for a job, loan or some other purpose, think twice! This could be a well-planned trap, which may land you in debt.

The same has happened with Sunil Sharma (30), a resident of Bhagat Road, whose identity proofs were tampered with by photos logging another person's photographs and were used to take six loans worth ₹4 lakh from three banks and three finance companies.

In conversation with Jitendra Thakur, Sunil said he received a call from the loan department of XCCI Bank after days back regarding a two-wheeler loan. He said he informed the bank official that he never availed



This suspect (in red jacket) was a key of two-wheeler that he purchased in India for name earlier tampering with his identity proofs to secure loans.



Tampered Aadhaar and PAN cards of Sunil Sharma.

## IDENTITY THEFT CASES BE COMING COMMON IN INDIA

A recent police awareness report has revealed that identity theft is on the rise in the country. In many cases, the fraudsters are using the identity of the victim to take loans and other financial services. The report also highlights the need for citizens to be more vigilant and to report any suspicious activity to the police.

## NEVER SHARE YOUR IDENTITY PROOFS WITH UNKNOWN PEOPLE

As per official data, one should be very careful while using mobile phones and laptops for online banking and other financial services. One should never share their identity proofs with unknown people. Even if one gets to take out a print of their identity proof, he must ensure they get deleted from the shop owner's computer, he added.

the same, I got to know that not just one, rather six such loans have been availed of in my name, which I never applied for," he added.

Sunil said "When I inquired about these loans from bank branches and finance companies concerned, I got to know that five two-wheeler loans and one consumer loan of ₹50,000 had been taken in my name. Then I filed an online complaint to the banks and finance companies informing them about the fraud and requested them to share CCTV footage of the person concerned, who visited them."

On the basis of the details shared by the bank employees and the groundwork he did, he got to know someone named Rahul was allegedly involved in this. He first opened a savings account in my name by using my identity proofs that had my name and details but someone else's photo and then used the same account number to avail other loans, he added.

"I then also realised that I had sent my Aadhaar and PAN card pictures on WhatsApp to my colleague's friend for job purpose, who further forwarded it to someone he contacted. I thought that it's him only who had tampered with my identity proofs," he added.

He has already filed an FIR against the unidentified person and shared all the details with the police. "The police have assured me that all those involved in the fraud would be arrested soon and my name would be deleted from all the records," he added.

Meanwhile, the ACP (Security) has confirmed that a complaint has been received and the investigation is underway to trace the accused.

# IDENTITY THEFT

- The two women received the cards on the addresses of their bungalows last week
- They were surprised to see photographs of different women and mismatch in dates of birth
- Their names and addresses were correct
- They reported the matter



Police found the cards were made at an Aadhaar centre in Junnar

to the cybercrime cell

- The police traced the women, whose photos were on the cloned cards
- These women said the suspect had asked them to pose for the photographs

# Bank executive held for identity theft, novel fraud

He used fake credentials to siphon money with a credit card

# FBI takes down marketplace that sold millions of stolen identities

Seventeen countries took part in the seizure and more than 100 were arrested.

APR 5, 2023

## FORGING DOCUMENTS

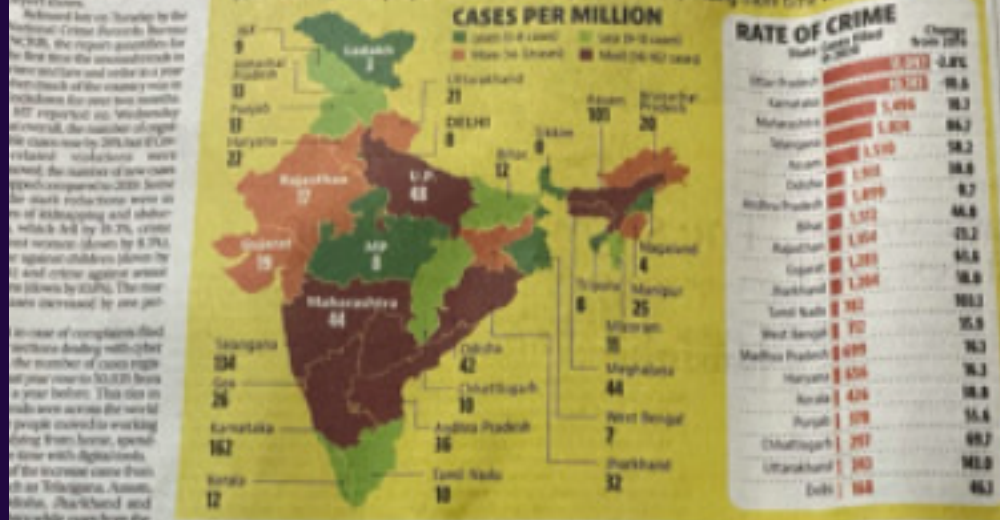
● The accused made 7,000 illegal Aadhaar card enrolments/ data changes by uploading forged documents

● To carry out enrolments and corrections in Aadhaar cards, the accused procured 6 Aadhaar kits comprising laptops, iris and fingerprint scanners and cameras



# Cyber crime registered 11.8% increase last yr: NCRB report

Number of cases filed last year under sections dealing with cyber crime rose to 50,000 from 44,775 a year before as more people moved to working from home, spending more time with digital tools



The report also highlights the need for citizens to be more vigilant and to report any suspicious activity to the police. It also mentions that the police have taken steps to improve their response to cyber crime cases, including the establishment of cyber crime cells in various states.

# ABOUT ME

**GAURAV TODWAL - SDE, MINIORANGE**

**Cyber Security Researcher and Identity Management Enthusiast**

**Passionate in Unraveling Why and How**



# THE BATTLE AGAINST DIGITAL IDENTITY THEFT

Presented By: Gaurav Todwal, miniOrange

# WHAT IS DIGITAL IDENTITY

Digital Identity encompasses the digital representation of individuals, organisations, or entities within the online realm. It comprises a collection of attributes, credentials, and characteristics that uniquely identify and distinguish a user in the digital space.





# THE SHADOW SELF: UNDERSTANDING DIGITAL IDENTITY THEFT





Who are you ?



Yu



No not me, you !



Yes, i'm Yu



Are you Deaf ?



No, Yu is Blind.



i'm not blind. You Blind.



That is what i just said !



# TYPES OF IDENTITY THEFT

## Financial

---

The most common culprit involves stolen personal information (think Social Security numbers, credit card details) used for unauthorized charges or even opening new accounts in your name.

## Office

---

Using your information to secure jobs or claim unemployment benefits can damage your employment history and reputation.

## Medical

---

Stealing your data for medical services or prescriptions in your name creates a nightmare scenario. Inaccurate medical records, denied insurance claims, and financial burdens are just some of the potential harms.

## Passport

---

Stolen passport information can be used for illegal travel or visa applications, putting your identity and safety at risk.

## Child

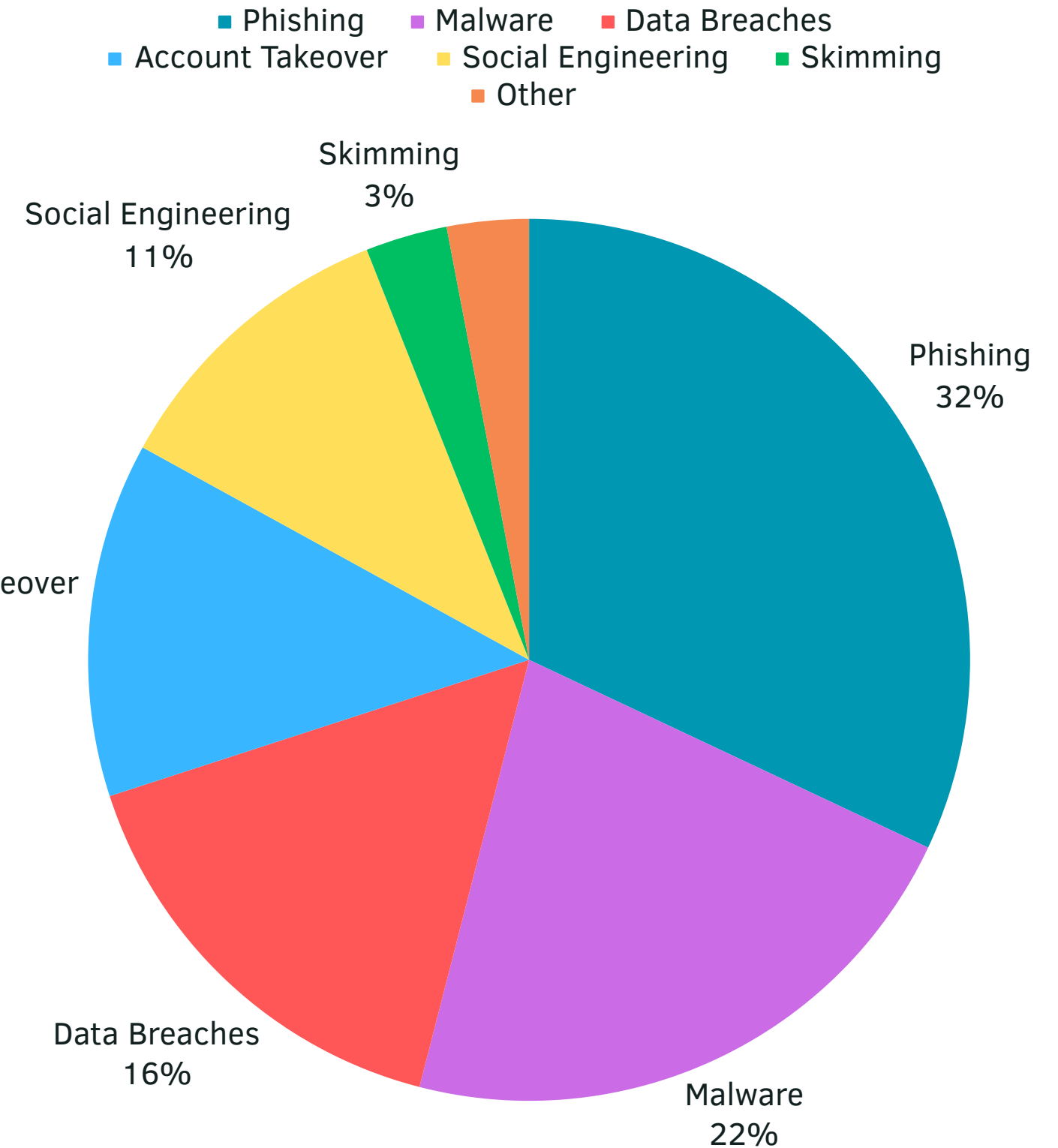
---

Children are especially vulnerable to identity theft, with stolen information used for opening accounts and causing long-term damage.

# HOW ARE IDENTITIES STOLEN?

As of November 2023

By understanding these hacking methods, you can build formidable defenses around your digital treasure chest.





# HAS YOUR DATA BEEN COMPROMISED?



';--have  
i been  
pwned?

**Have I Been Pwned: Check if your email has been compromised in a data breach**

Have I Been Pwned allows you to search across multiple data breaches to see if your email address...

[haveibeenpwned.com](https://haveibeenpwned.com)

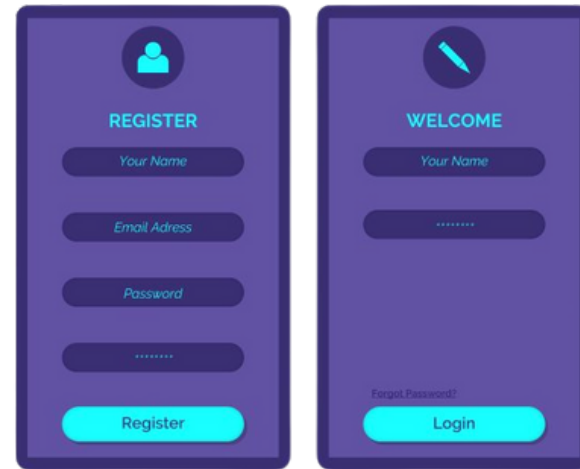


# FROM DATA BREACH TO BUILDING DATA FORTRESS

Let's understand how we can build the unbreakable fortress to safeguard our identity.

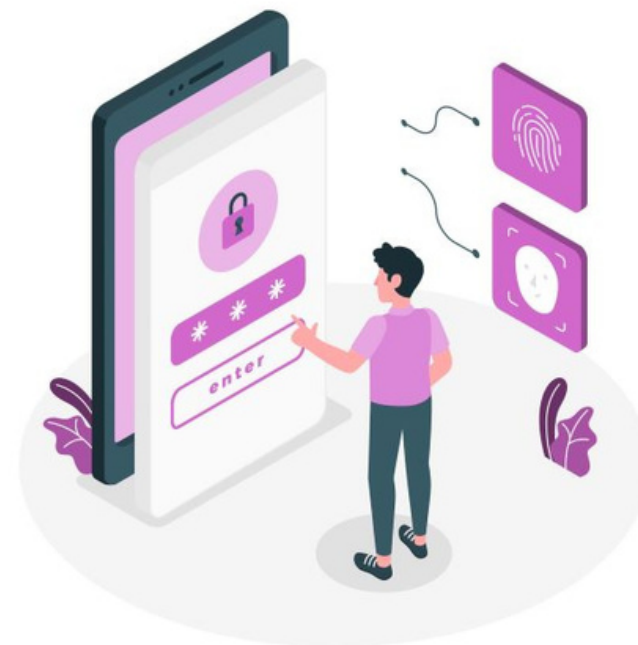


# Centralized Identity



- Using the username and password to login into the sites or sites
- The bad player if had access to your password he can access any of your data.
- **Why to shift:** Password vulnerability
- **Where to shift:** Password Vault and Single Sign-On.

# Federated Identity



- Arose when Web and Software as a Service were seeing broad adoption and password protection.
- User data is stored with an unknown federated source.
- **Why to shift:** Privacy and data protection
- **Where to shift:** Decentralized sources of authentication.

**WHAT IS**

**DECENTRALIZED IDENTITY (DID)**



# Let's **Touch** the Surface of **DID**:

## Individual Control and Enabling Trust

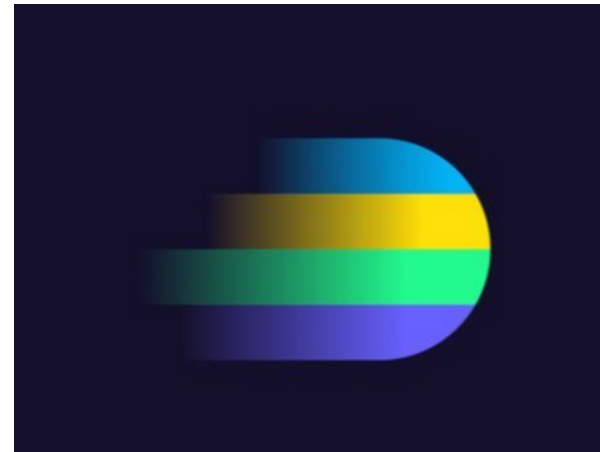
Decentralized identity gives the individual control over their own identity, so that they can decide how their personal information is shared and accessed, enabling trusted interactions while preserving privacy.



# LET'S UNDERSTAND WITH AN **EXAMPLE**

You, Aadhar and Airport Authority of India

# UNDERSTANDING WITH EXAMPLE

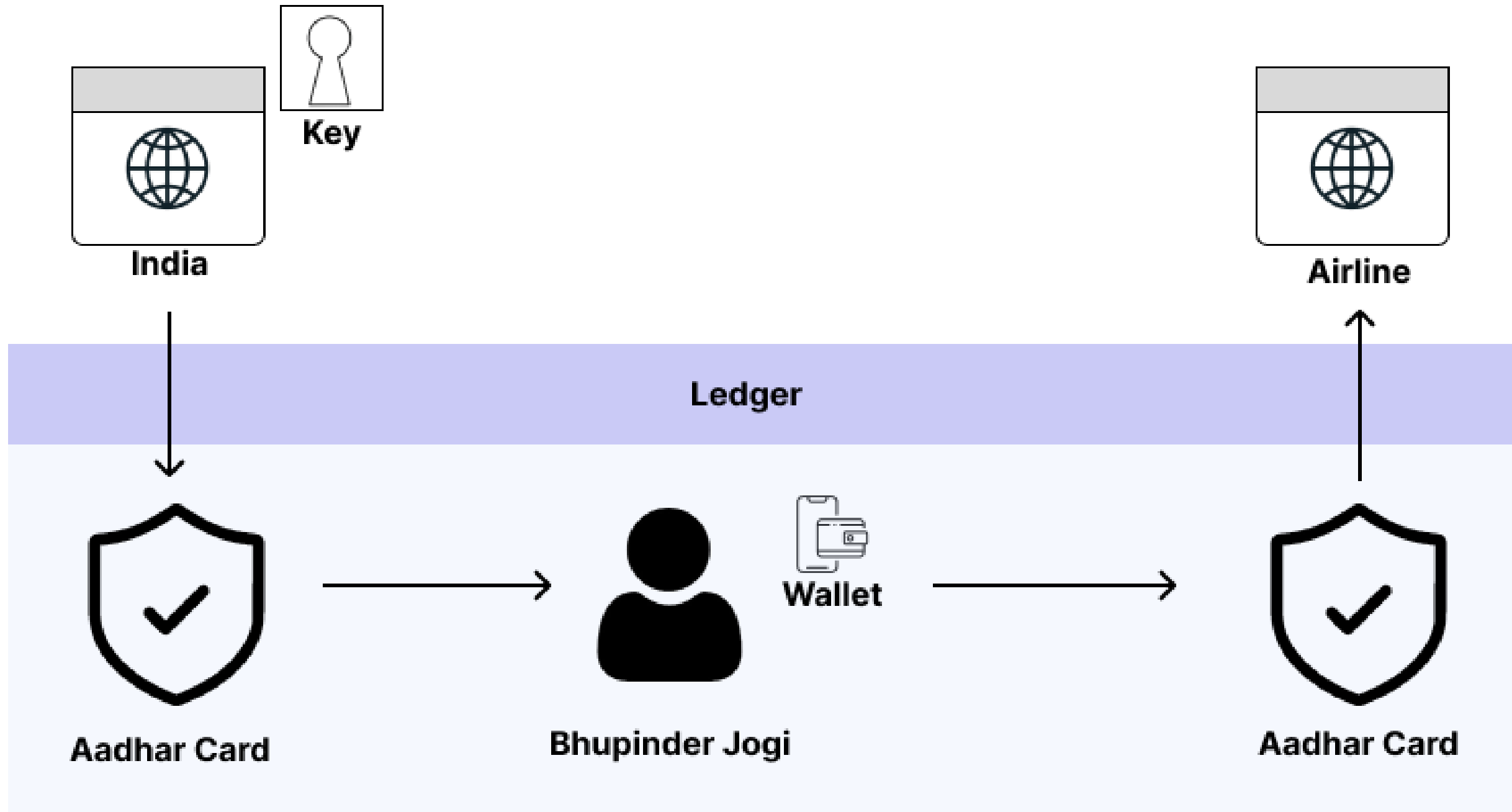


**Issuer**

**Holder**

**Verifier**

# BASIC SETUP

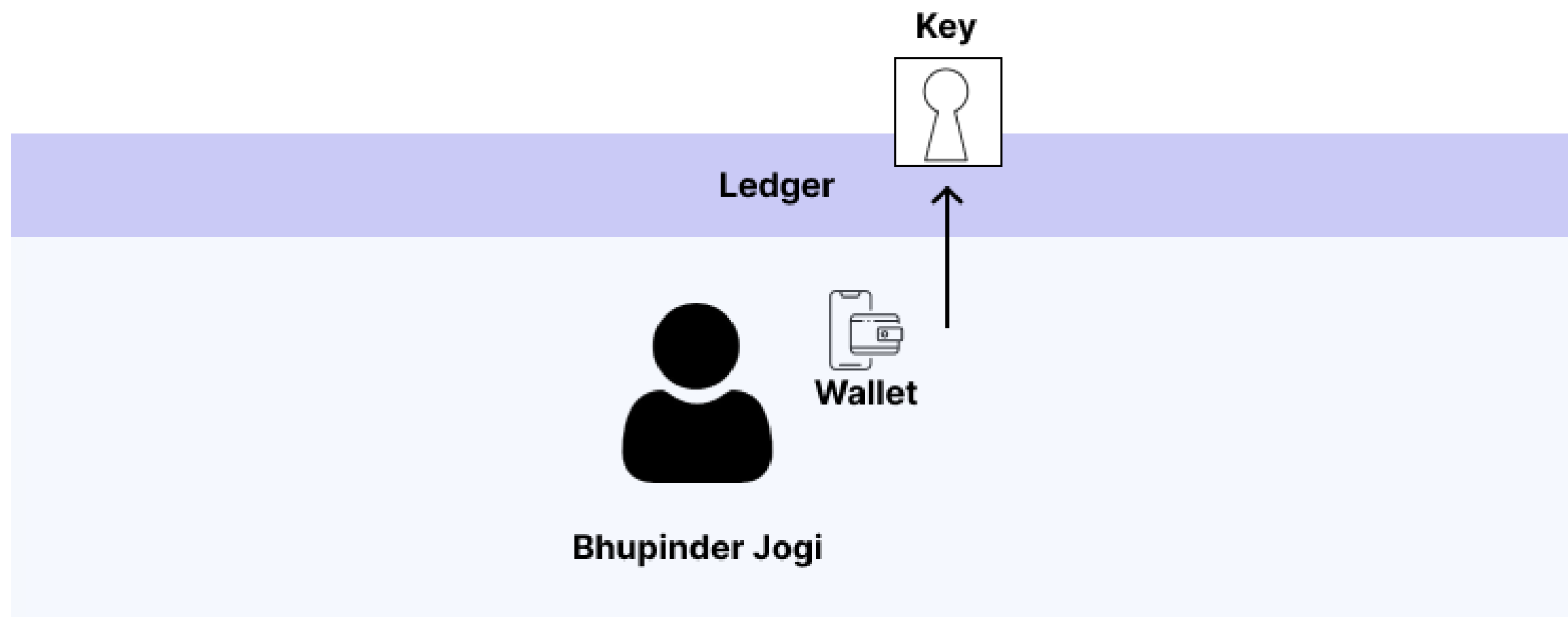


Let's see how **Bupinder Jogi**, will obtain and user **Digital Identity**:

- Bupinder Jogi will install the identity wallet.
- He requests for the Identity which will be installed in his wallet.
- Jogi presents his digital identity to any of the Airport Authority.
- Airport Authority before providing the service will validate the identity and confirm its belonging.



# CREATE IDENTITY



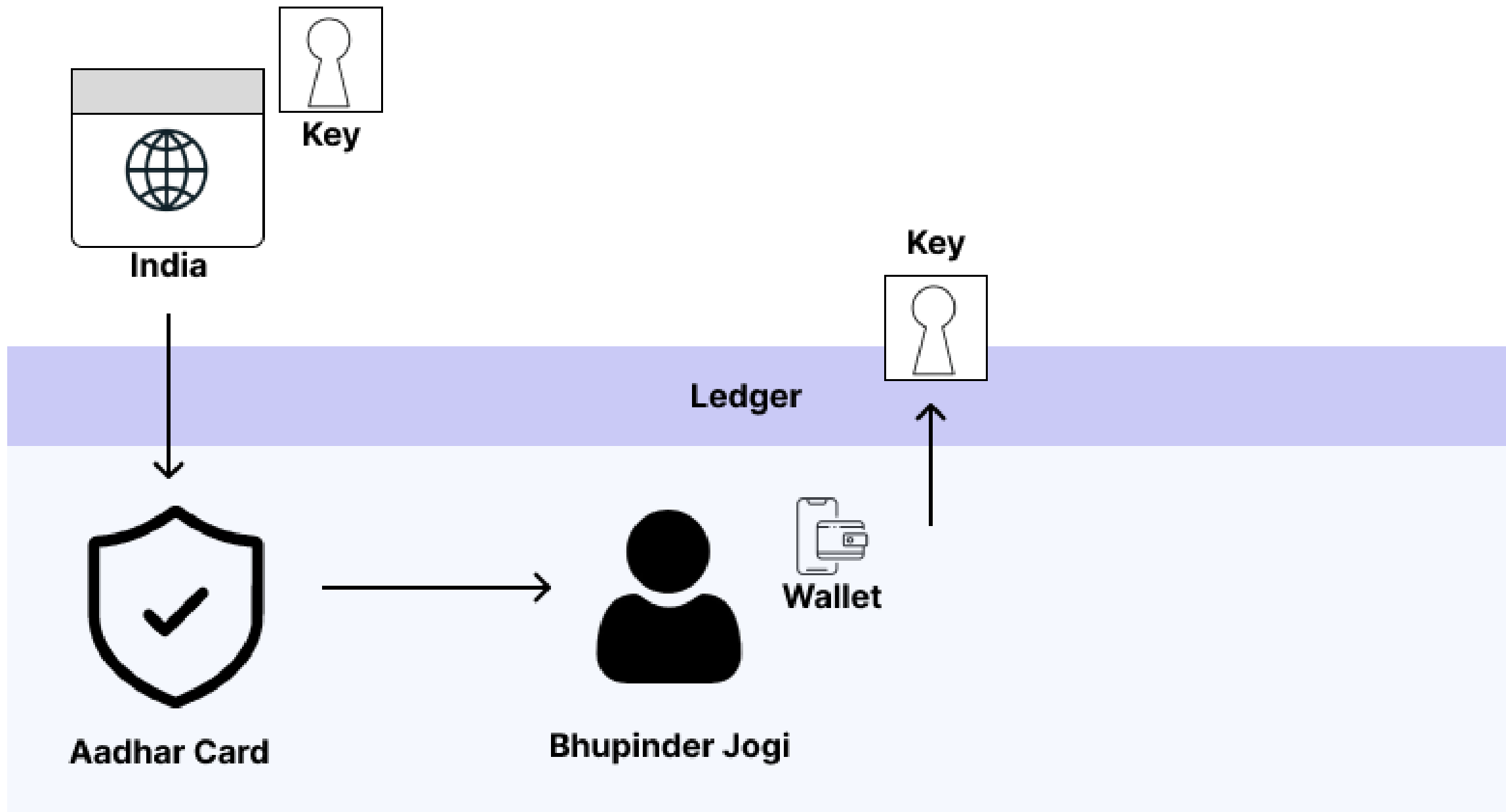
The wallet generates an identifier for Jogi along with key pair that is used to prove ownership of the identifier.

The private key is stored in the wallet and in return, the public key is published to the ledger.

Identifier will be used to identify the Jogi in this Digital Ecosystem.

The key will be used to verify the Jogi's identity.

# FETCHING THE DOCUMENT



Now that our identity wallet is configured, Jogi request the documents like Aadhar Card, Driving license, etc from the Indian Government.

After being issued the digital document will be stored inside the wallet.

With just a single click , the document is seamlessly issued and stored in her wallet using the new Web API's

# DIGITAL DOCUMENT

Issuer: Indian Authority

Subject: Bhupinder Jogi  
DOB: 19-05-1978

*Govt. of India*

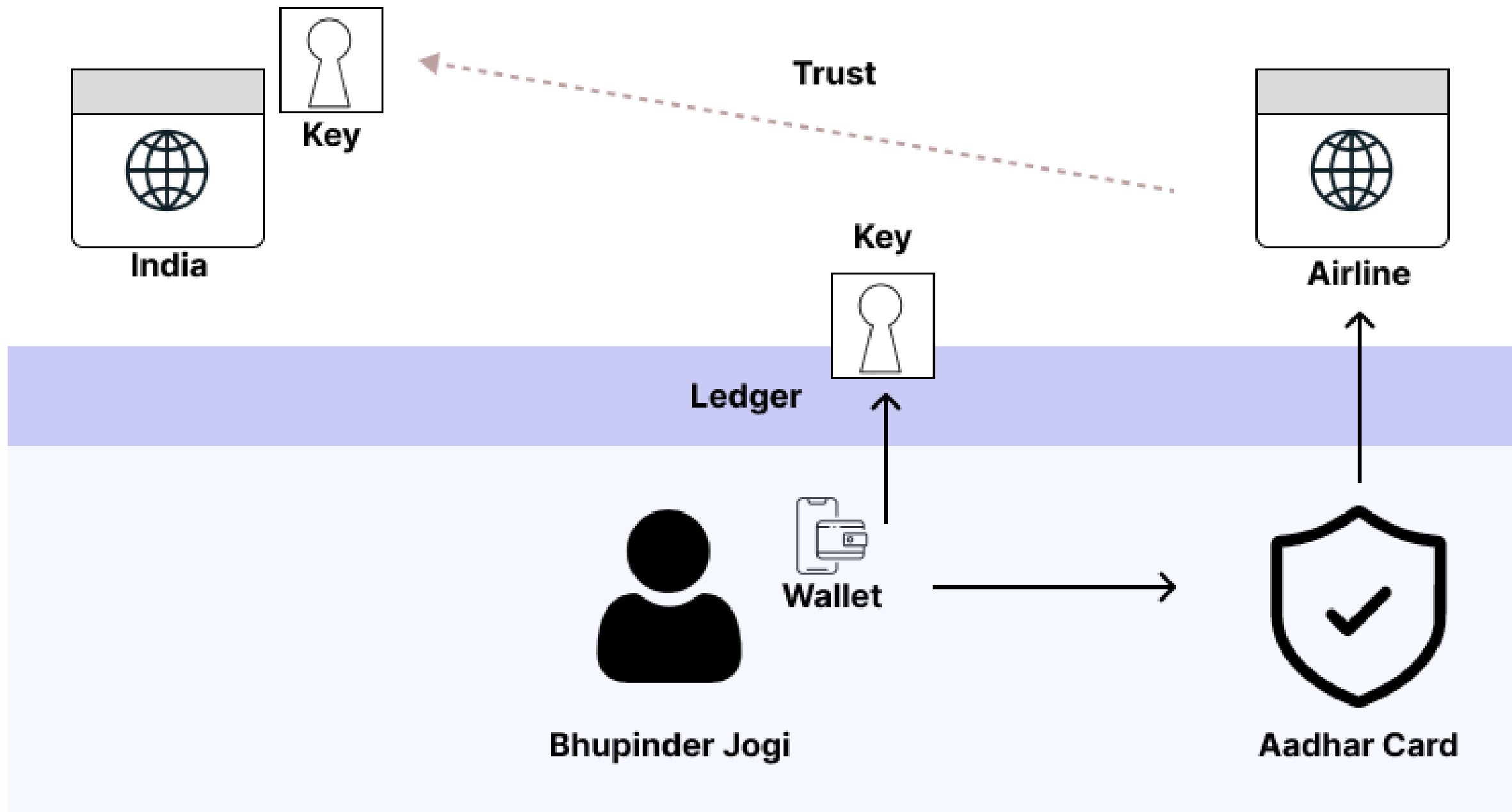
Digital Document Contains three major component:

1. Issuer
2. User claims
3. Signature

The signature can be used to validate the document is issued by trusted source or not.

This signature is equivalent to the anti-tempering measures present in our physical passport.

# VERIFYING THE DOCUMENT



Just as the federated identity (SAML and OAuth) the service provider or verifier had a trust relationship with the Issuer.

The trust relationship configures the information about where the public key is stored

The public key is used to verify signature and verify the authority of the document

# AADHAR PRESENTATION:

Issuer: Indian Authority

Subject: Bhupinder Jogi  
DOB: 19-05-1978

*Govt. of India*

*Bhupinder*

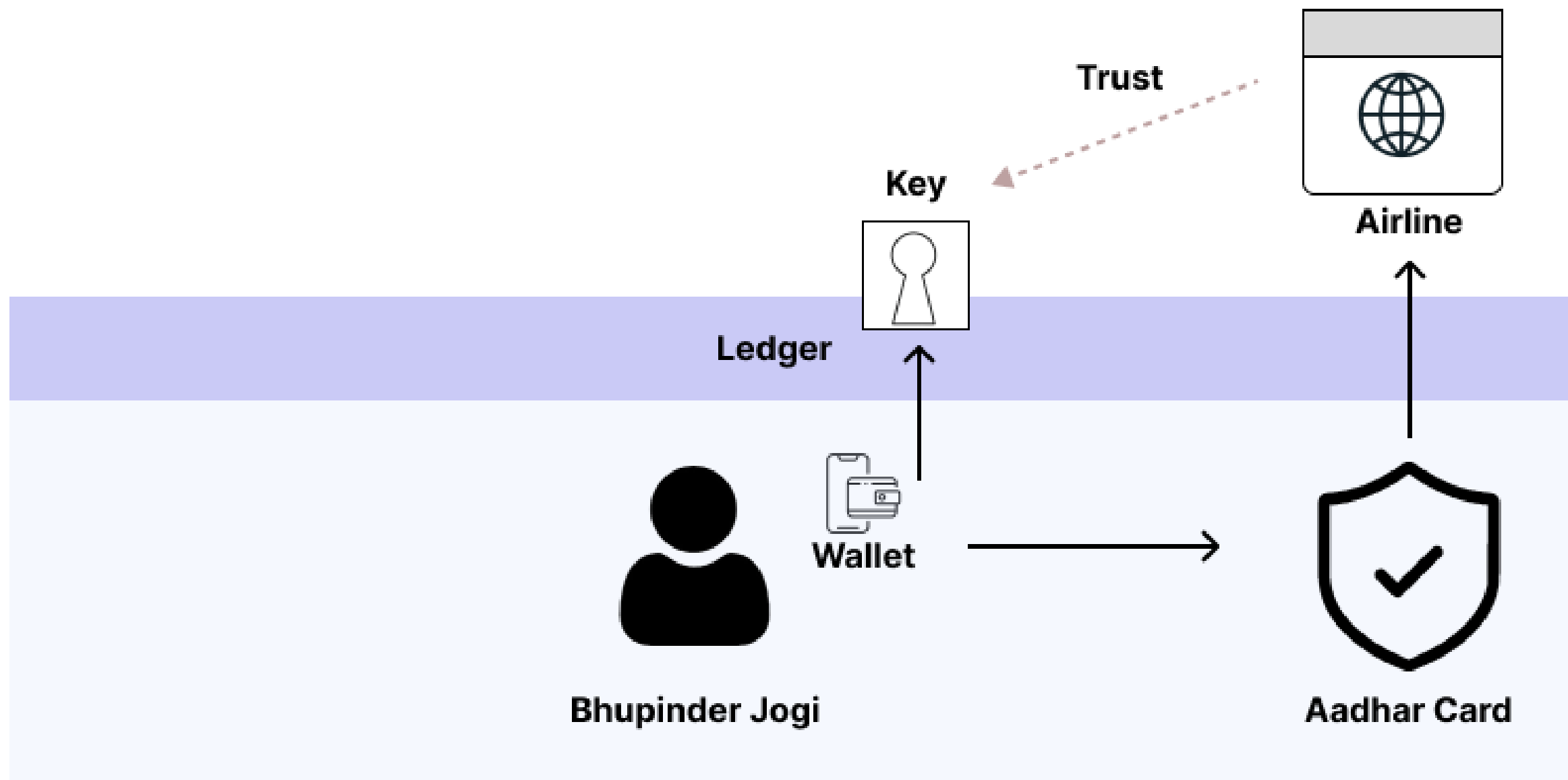
The Aadhar itself is encompassed by another digital signature from the wallet.

This will allow the service provider to verify two things:

1. The ID is issued from the correct authority
2. The person presenting the ID is the legit person or not

Verifying the holder signature will require the holder's public key

# VERIFYING HOLDER



This bring us to the end of this Digital System ecosystem.

The public key registered on the ledger will be required to verify the holder's identity.

After being verified, the service provider can now allow the holder to access the service.

# HOW WE ARE CONTROLLING OUR IDENTITY?

# SELF-SIGNED CREDENTIALS



Issuer: Bhupinder Jogi

Subject: Bhupinder Jogi  
Fav Movie: Bhupinder

*Bhupinder*

Users can now choose to issue Self-Signed credentials about themselves that don't need to be made by the third party

This functionality was unavailable in the Federated Identity system because the user has no cryptographic keys only the website does.

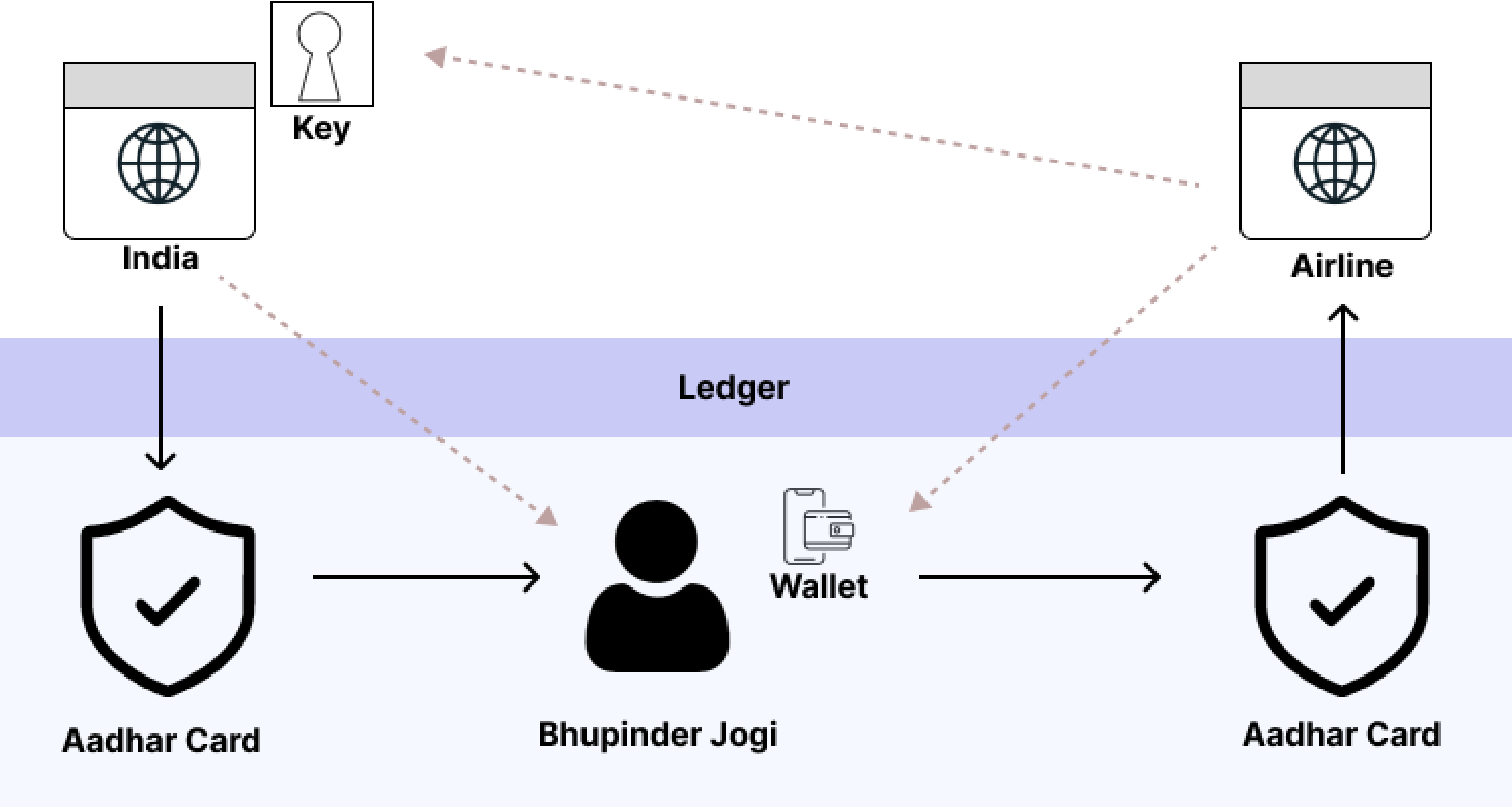
The cryptographic keys are the major requirement to generate the Verifiable credentials.

This notion of the self-signed credentials give the rise to the term Self-Soverign Identity

Transfer of the credentials is in control of the holder who is showcasing the identity

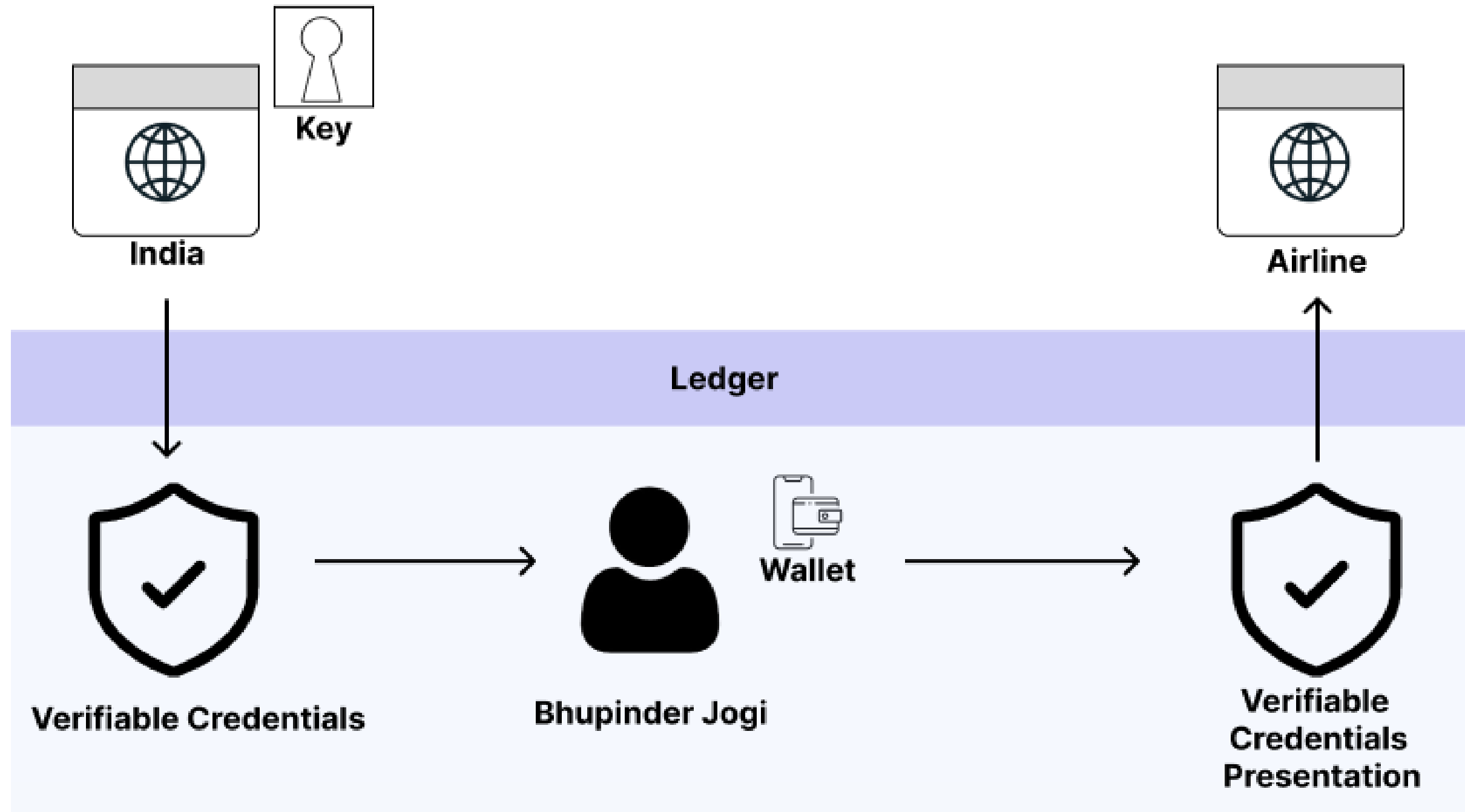


# TRUST TRIANGLE



# LET'S DIG DEEP INTO DECENTRALIZED IDENTITY ECOSYSTEM

# THE ECOSYSTEM



The major actors in the Decentralized Identity Ecosystem are:

1. Wallet
2. Ledger
3. Verifiable Credentials

# DIGITAL WALLET



Wallet are the application which allows the user to manage and control there identity.

The main function of the wallet is to manage the identifiers and cryptographic key associated with those identifiers.

Wallet also manages the keys and information published on the distributed ledger.

Exchanging of the verifiable credentials with issuer and verifier is managed through the wallet.

# DECENTRALIZED IDENTIFIERS

**did:ethr:dfv-gtak-pab7-jen7-p4e**

Decentralized Identifiers are globally unique and don't require any central registeries.

DID contains three major part:

1. Prefix
2. Method (Ledger)
3. Identifier

DID is resolvable and its ownership can be proven with the public key cryptography.

# LEDGERS



**did:btcr**



**did:ethr**



**did:sov**



**did:ipid**



**did:ion**



**did:peer**

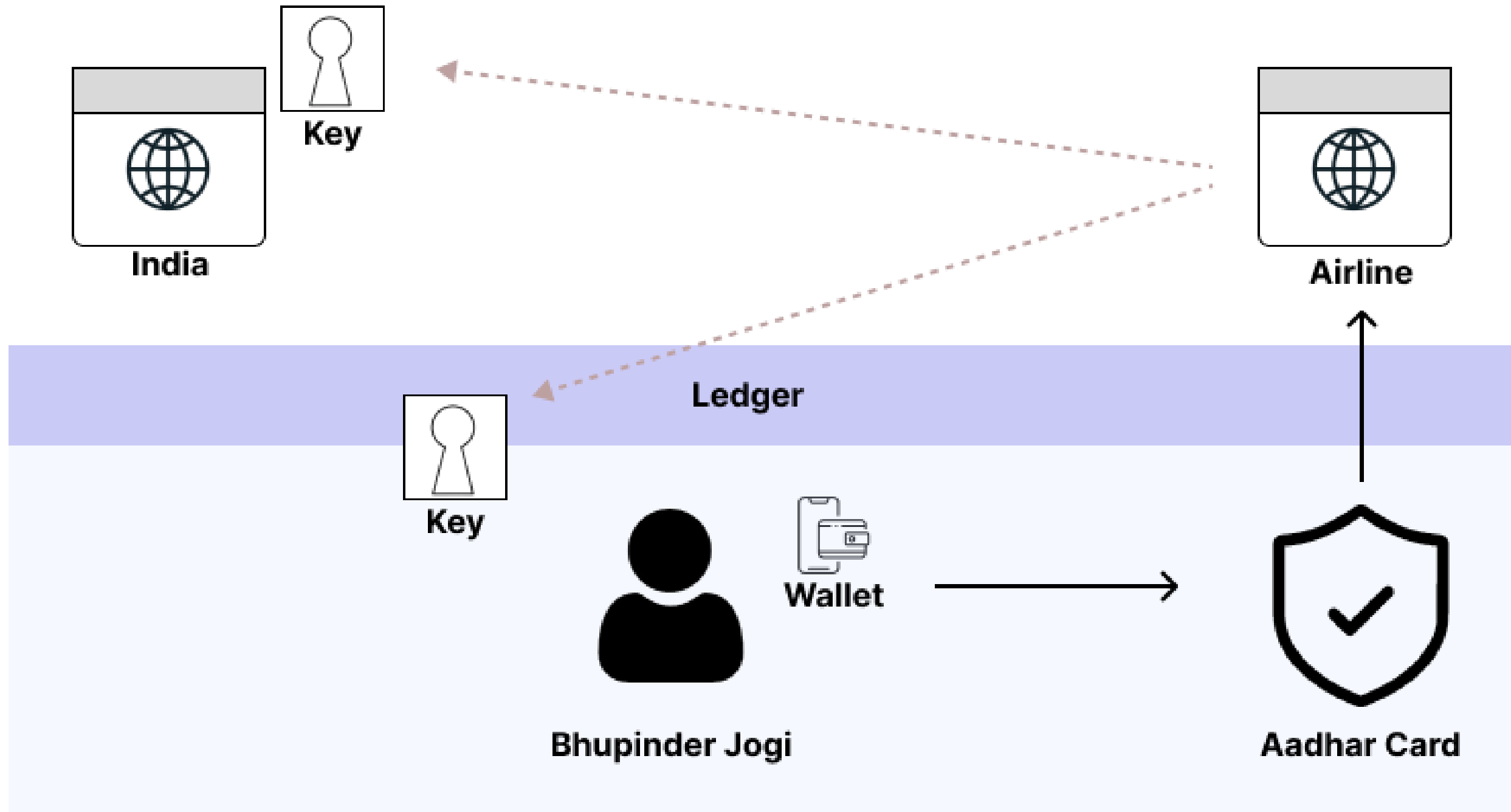
Wallet, in addition of storing credentials, keys and secrets also publishes an individual public keys to the ledger.

Ledgers helps in making the decentralized ecosystem network centric.

The method contained in DID will specify how to publish, update and deactivate the identifier on the ledger.

Create, Update and Delete functionality is performed by individual through the wallet.

# VERIFYING CREDENTIALS



Verifying a credentials requires a public key, need to validate the digital signature on the credential

# WHAT'S NEXT ?





# TAKE AWAY:





WE VALUE YOUR **FEEDBACK**

Connect with me.



+91 8949461981



[gaurav.todwal@x securify.com](mailto:gaurav.todwal@x securify.com)



[gauravtodwal](https://www.linkedin.com/in/gauravtodwal)

