Proof Invisibility

Let's build a decentralized *almost invisible* event attendance system

Decentralized Event Network Node for Intelligent Supervision

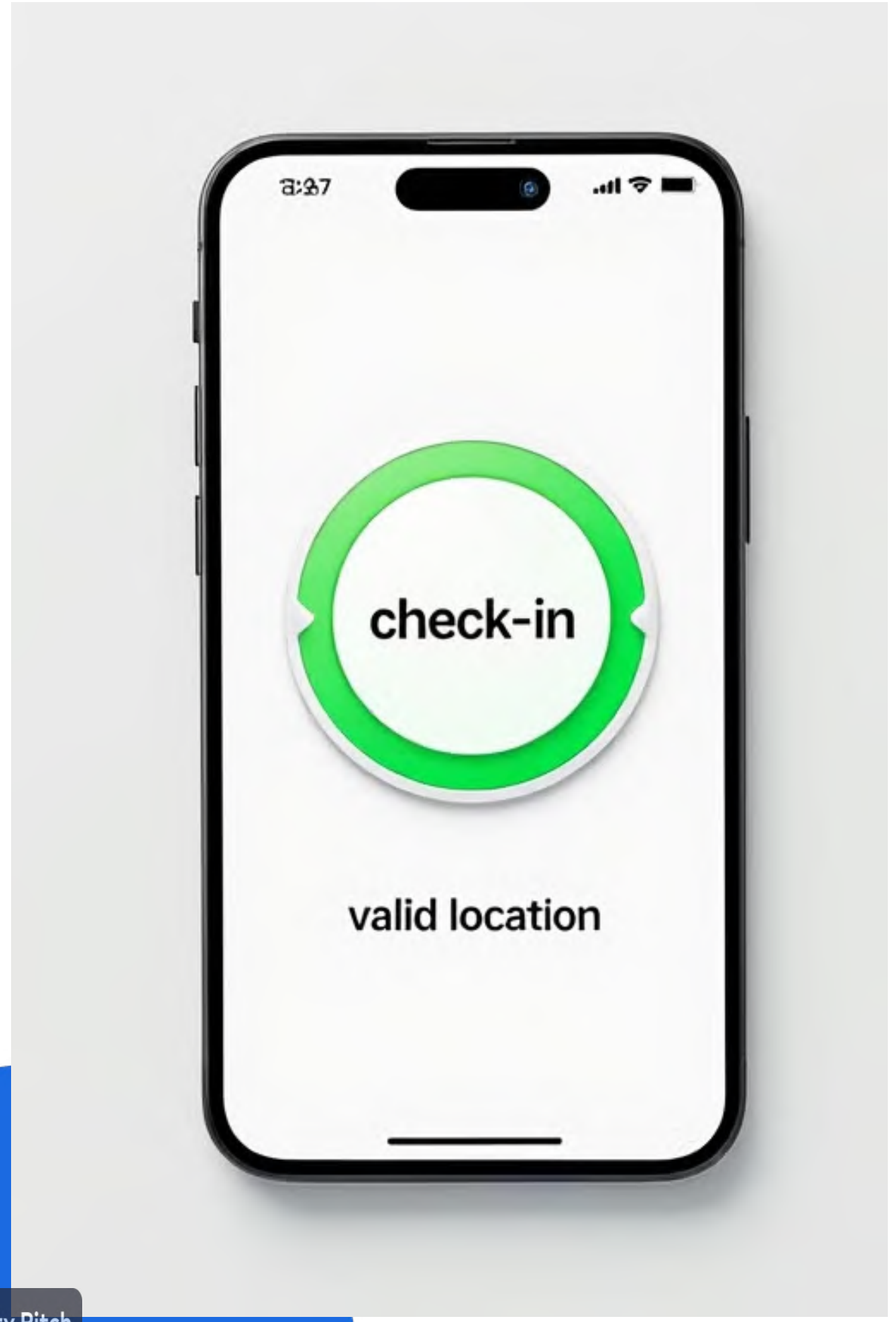
Was known as

DENNIS

Masked Identity Check-ins with Cryptographic Knowledge Yield

Now known as

MICKY



Overview: Privacy-Preserving Automated Check-In System

Purpose: To track office or event attendance using zero-knowledge proofs (ZK proofs) to protect user privacy.

Key Components:

- **NFC Device**: Verifies physical presence and provides valid data.
- **Check-in App**: Simplifies check-in for users via mobile devices with simple App.
- **Zero-Knowledge Proofs**: Ensures attendance is recorded without revealing user data.

Comparison of Verification Methods

The key points of the verification are people, location, attendance...

WiFi Verification:

- Simple but can be spoofed by duplicating network SSID.
- Requires additional hardware (WiFi routers).

GPS Geofencing:

- Easy to implement and widely supported.
- Susceptible to spoofing, making the data less trustworthy.

NFC Verification*(Selected)*:

- Secure and physical, but requires users to tap an NFC tag.
- Ensures precise location verification and provides reliable data for proof generation..

Technical Architecture

Frontend (local device):

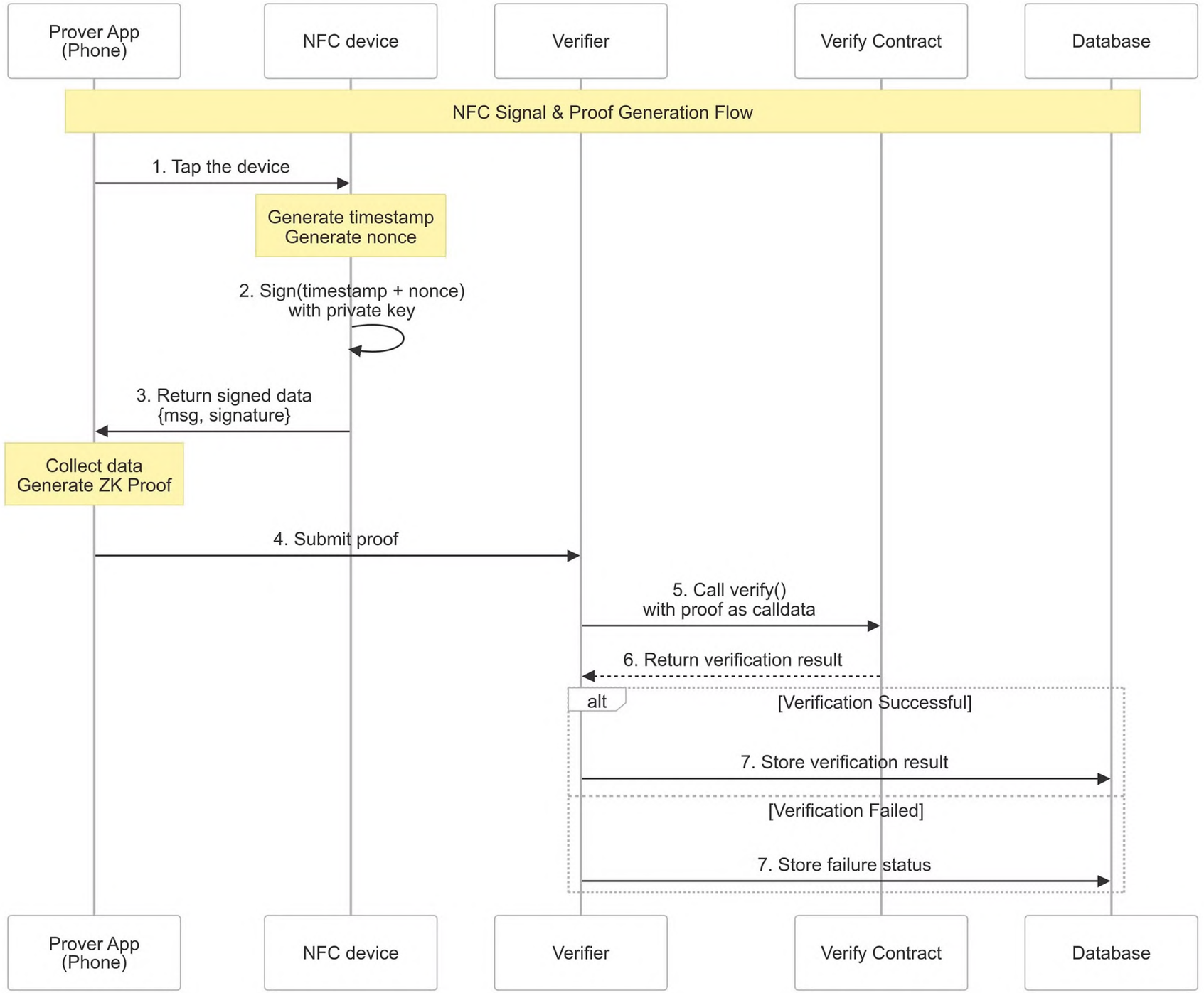
- simple app to interact with NFC device to make location verification and check-ins.
- generate proof and send to verifier.

Backend:

- verifying ZK proofs (attendance record).

Security:

- Proof of attendance is stored on the server, but personal data remains private through ZK proofs.


Prover App (Phone)
NFC device
Verifier
Verify Contract
Database
NFC Signal & Proof Generation Flow
1. Tap the device
Generate timestamp
Generate nonce
2. Sign(timestamp + nonce) with private key
3. Return signed data {msg, signature}
Collect data
Generate ZK Proof
4. Submit proof
5. Call verify() with proof as calldata
6. Return verification result
alt
[Verification Successful]
7. Store verification result
[Verification Failed]
7. Store failure status
Prover App (Phone)
NFC device
Verifier
Verify Contract
Database

Pitch

Want to make a presentation like this one?

Start with a fully customizable template, create a beautiful deck in minutes, then easily share it with anyone.

Create a presentation (It's free)