HaRBInger 2025

Innovation for Transformation

TrustKYC Vault

Tokenised, Consent-Driven Digital KYC for Secure Financial Ecosystem

Presented By:

- Reema Srivastava — Project Leader - 9120758672
- Shubham Kumar Vishnoi — Team Member - 9058612403

☐ **Technology Focus:** .NET Development

TrustKYC Vault

|

| Tokenised, Consent-Driven Digital KYC |

| for Secure Financial Ecosystem

TrustKYC: Tokenised, Consent-Driven Digital KYC for India

- ✔ Project Name: **TrustKYC**
- ✔ Team Name: AI Innovation Team
- ✔ Team Members: 2 Member
- ✔ Submission Category: **Theme 1 — Tokenised KYC**

Slide 2 — Problem Background & Why It Matters

Today in India, every bank, wallet, insurance provider, and financial application requires a separate KYC process.

This results in:

User onboarding friction

Repeated verification cost

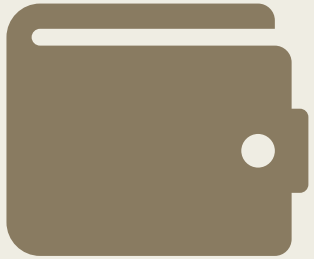
Higher risk of identity exposure & data leaks

Slow digital financial inclusion

Repeated KYC effort = Over ₹100 crore annual cost to the financial ecosystem (estimated)

SLIDE 3 — GAP ANALYSIS: WHAT'S MISSING TODAY?

Current System	Issue
Separate KYC for each institution	Redundant and costly
Aadhaar + OTP Model	No selective disclosure
Identity stored across multiple systems	Higher breach risk
No unified consent mechanism	Lack of transparency & user control



Slide 4 — Vision Statement

“To create a reusable digital KYC identity token controlled by the user and accepted across all financial institutions in India.”

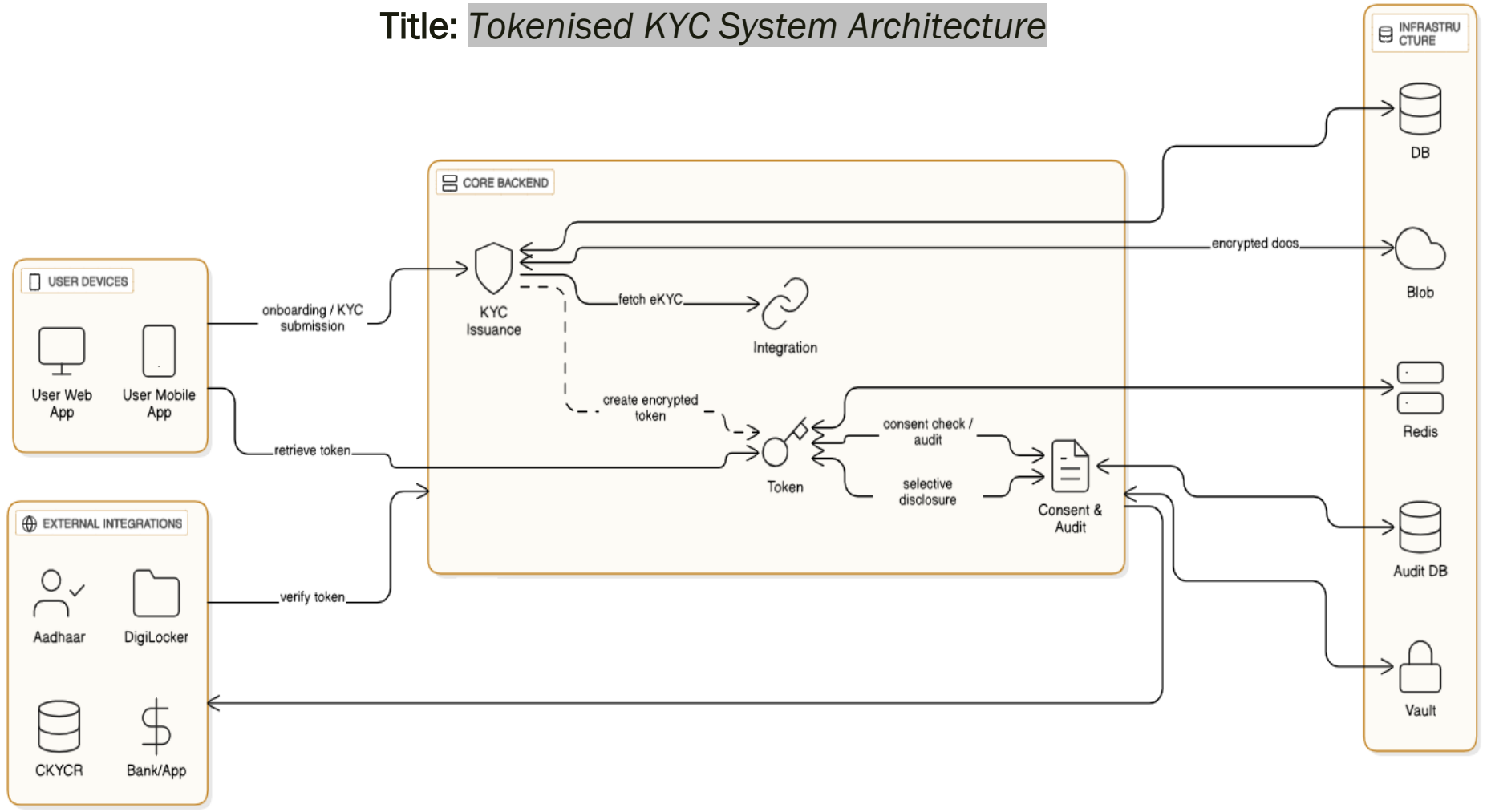
Slide 5 — Solution Concept: TrustKYC

Our solution introduces a secure and reusable KYC token model that supports:

- ✔ One-time KYC verification
- ✔ Secure encrypted identity tokens
- ✔ Consent-driven data sharing
- ✔ Tamper-proof verification with audit logs
- ✔ Interoperability with Aadhaar, DigiLocker, and CKYCR

Slide 6 — System Architecture

Title: *Tokenised KYC System Architecture*



Slide 7 — Workflow Summary	**User Onboarding**	Aadhaar / DigiLocker-based identity authentication	KYC verification completed
Encrypted TrustKYC token generated	**Sharing with a New Financial Institution**	User shares token	Institution verifies via TrustKYC API
Only required data is shared (**selective disclosure**)	**Update & Revocation**	Change in identity → Token updated	Updated record is reflected across institutions

SLIDE 8 — KEY FEATURES

ZERO-TRUST SECURITY MODEL

SELECTIVE DISCLOSURE WITH CONSENT CONTROL

PLUG-AND-PLAY API ECOSYSTEM

REUSABLE IDENTITY ACROSS INSTITUTIONS

FULL COMPLIANCE WITH CKYCR AND RBI GUIDELINES

SLIDE 9 — TECHNOLOGY STACK (.NET FOCUSED)

Layer	Technology
Backend Framework	ASP.NET Core 8 Web API
Authentication	OAuth2 + OpenID Connect + JWT
Database	PostgreSQL / SQL Server
Caching	Redis
Security	RSA/ECDSA + AES-256 Encryption
Token Format	JSON-LD + W3C Verifiable Credentials
Client App (Optional)	.NET MAUI
Cloud	Azure / AWS
Logging	Serilog + Seq

Slide 10 — Security Model

- Public-private key cryptography
- Secure key vault for signing and storage
- Token tamper detection and verification
- Support for **Zero-Knowledge Proofs (ZKP)** for privacy-preserving validation

Slide 11 — Compliance & Integration

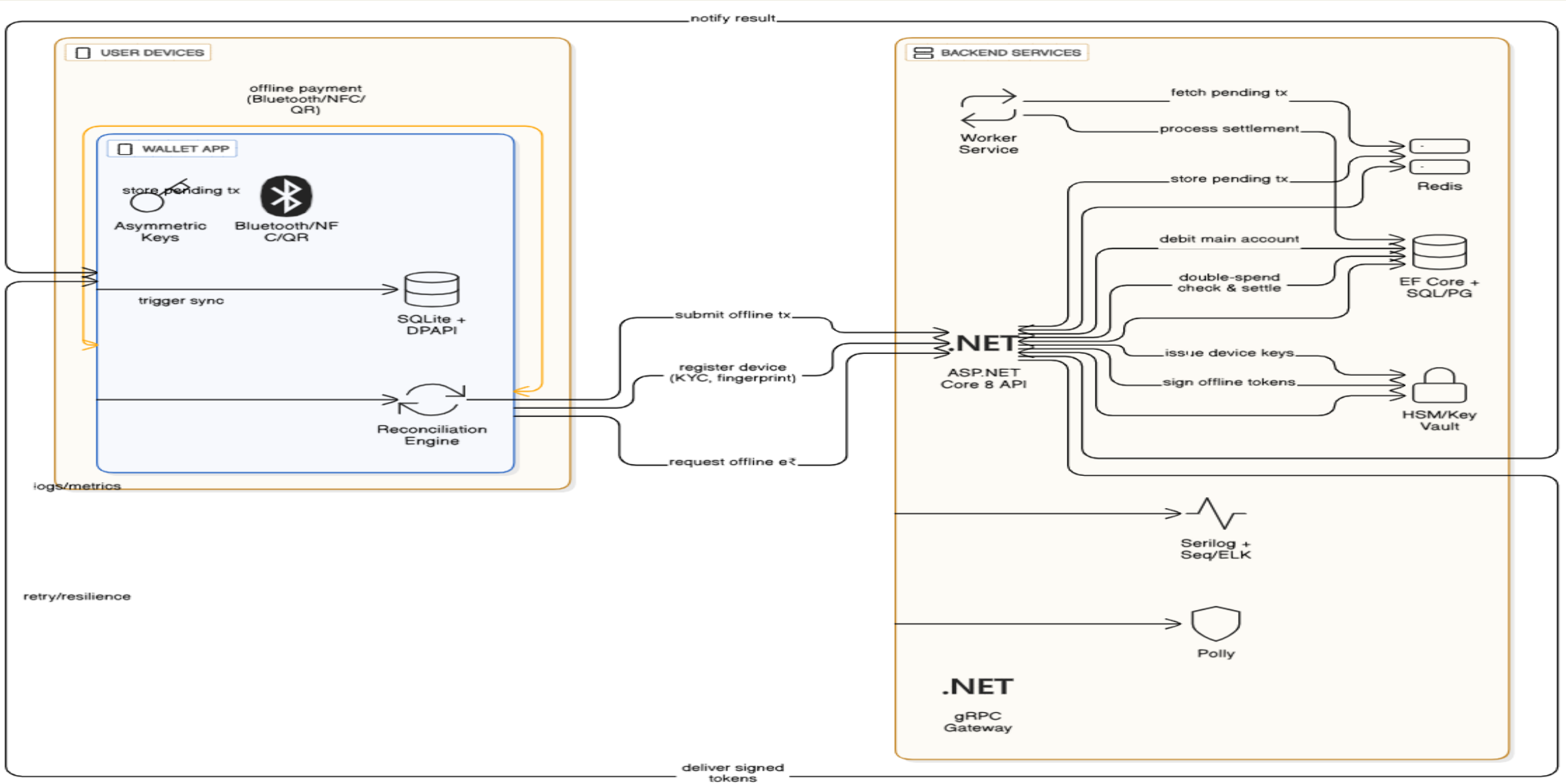
The system aligns with existing and upcoming Indian digital identity standards:

- Aadhaar Offline Verification
- DigiLocker API integration
- CKYCR dataset compliance
- India Data Protection Act & RBI Digital Identity Framework

Slide 12 — Business Impact & Scalability

- ✔ Reduction in repeated KYC processing cost
- ✔ Faster onboarding (seconds instead of days)
- ✔ Increased trust and fraud reduction
- ✔ National identity interoperability at scale

Slide 13 – Flow Chart Working Scenerios (Demo)



SLIDE 14 — ROADMAP

We are a dedicated and solution-driven team, and we are confident that we can complete this project even before the proposed timeline. We have already developed and launched multiple applications in the market, including wallet-based systems that support payments without the need for internet connectivity.

Given our experience and proven capability, if we are provided the opportunity, we will deliver this solution efficiently and in a significantly shorter time frame

Phase	Duration	Output
Prototype	30 Days	Working demo + Token API
Pilot	3–6 Months	Deployment with two FI partners + CKYCR integration
Scaling	1–2 Years	National adoption and ecosystem standardization

Slide 15 — What Can Our Team Deliver

Strong expertise in **.NET architecture and secure backend development**

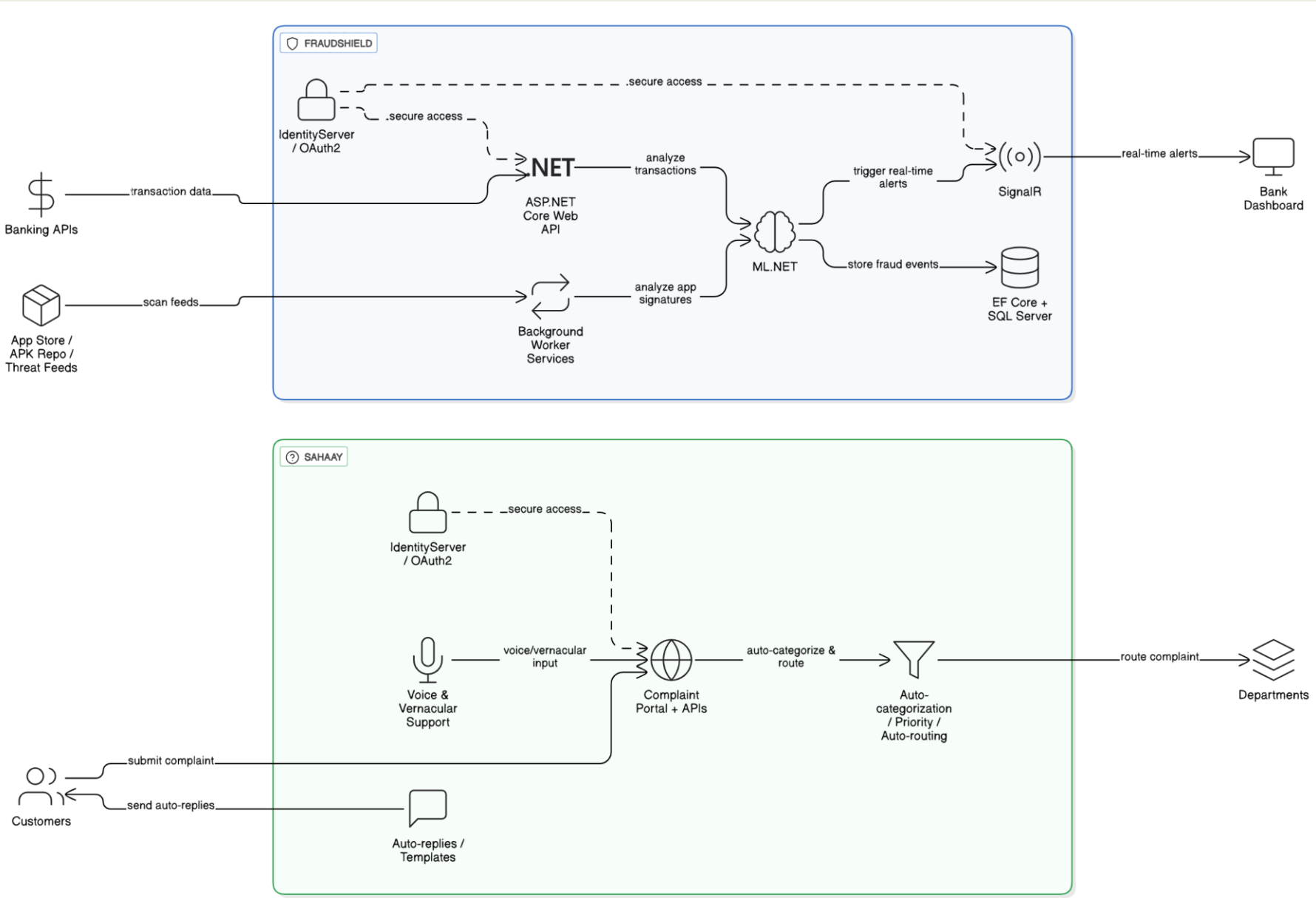
Hands-on experience in identity systems, APIs, and cryptography

Understanding of Aadhaar, DigiLocker, and digital public infrastructure

Experience building scalable enterprise-grade software

SLIDE 16 — FINAL MESSAGE

TRUSTKYC ENABLES SECURE, REUSABLE, AND CONSENT-DRIVEN IDENTITY VERIFICATION — BUILDING A MORE TRUSTED AND FRICTIONLESS DIGITAL FINANCIAL SYSTEM FOR INDIA.



NPCI

भारतीय राष्ट्रीय भुगतान निगम

NATIONAL PAYMENTS CORPORATION OF INDIA