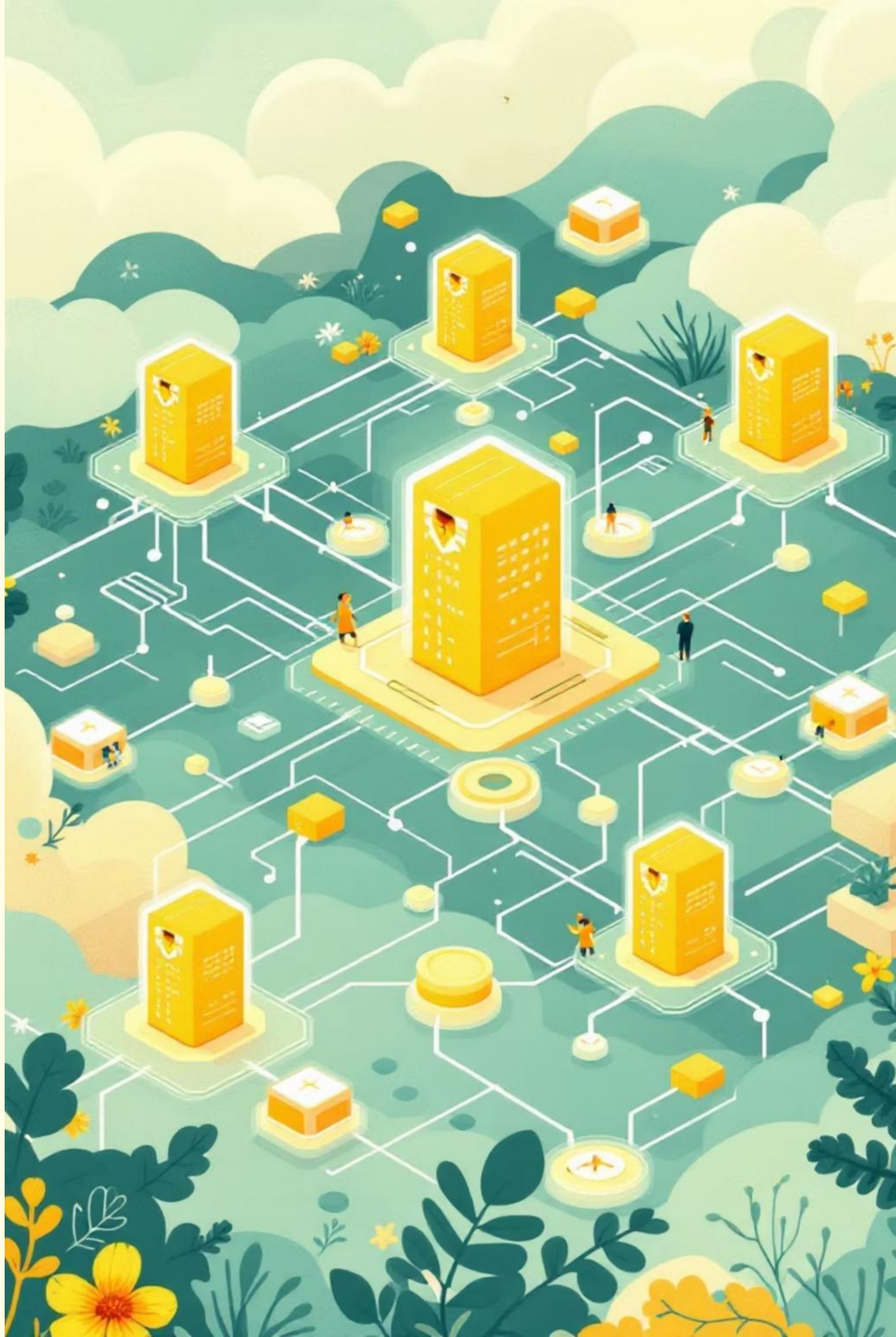
AI/ML based Confidential Computing Rooms: Fraud Prevention & Privacy-Preserving Data Collaboration

Unlocking the power of sensitive data through hardware-enforced privacy and real-time collaboration

YELLOWSENSE TECHNOLOGIES PVT LTD

tech@yellowsense.in



Details about the Company

Company Identification

Company Name: **YellowSense Technologies Pvt Ltd**

Startup India DP-IIT: DIPP 138 388

MSME Udyog Aadhar: **UDYAM-KR-03-0293956**

Startup Karnataka Reg No: KITS/SK-REGN/2023-24/3086

CIN No.: U62099KA2023PTC174648

TAN No.: BLRY02955B

PAN No.: AABCY6908P

Incorporation & Leadership

Date of Incorporation: 7th June 2023

Location: Bengaluru - KA

Directors:

Prakhar Goyal (50%) - DIN: 8467656

Komal Goyal (50%) - DIN: 10194464

Problem statement

Problem Statement
Fingerproofing
Fake
Fingerprint
YellowSense

Problem Statement (contd)

Data silos block innovation

Sensitive datasets (healthcare, finance, welfare) are fragmented.

Current scenario

- Regulators face >150 reported pump-and-dump cases in India in the past 2 years (SEBI).
- ₹1,000+ crore lost annually to welfare fraud & duplicate beneficiaries (CAG reports).
- 80% of healthcare data goes unused in clinical research (Frost & Sullivan, 2023).

What's done today

manual audits, delayed investigations, or restricted data sharing under NDAs. software-level encryption resulting in lower trust between parties

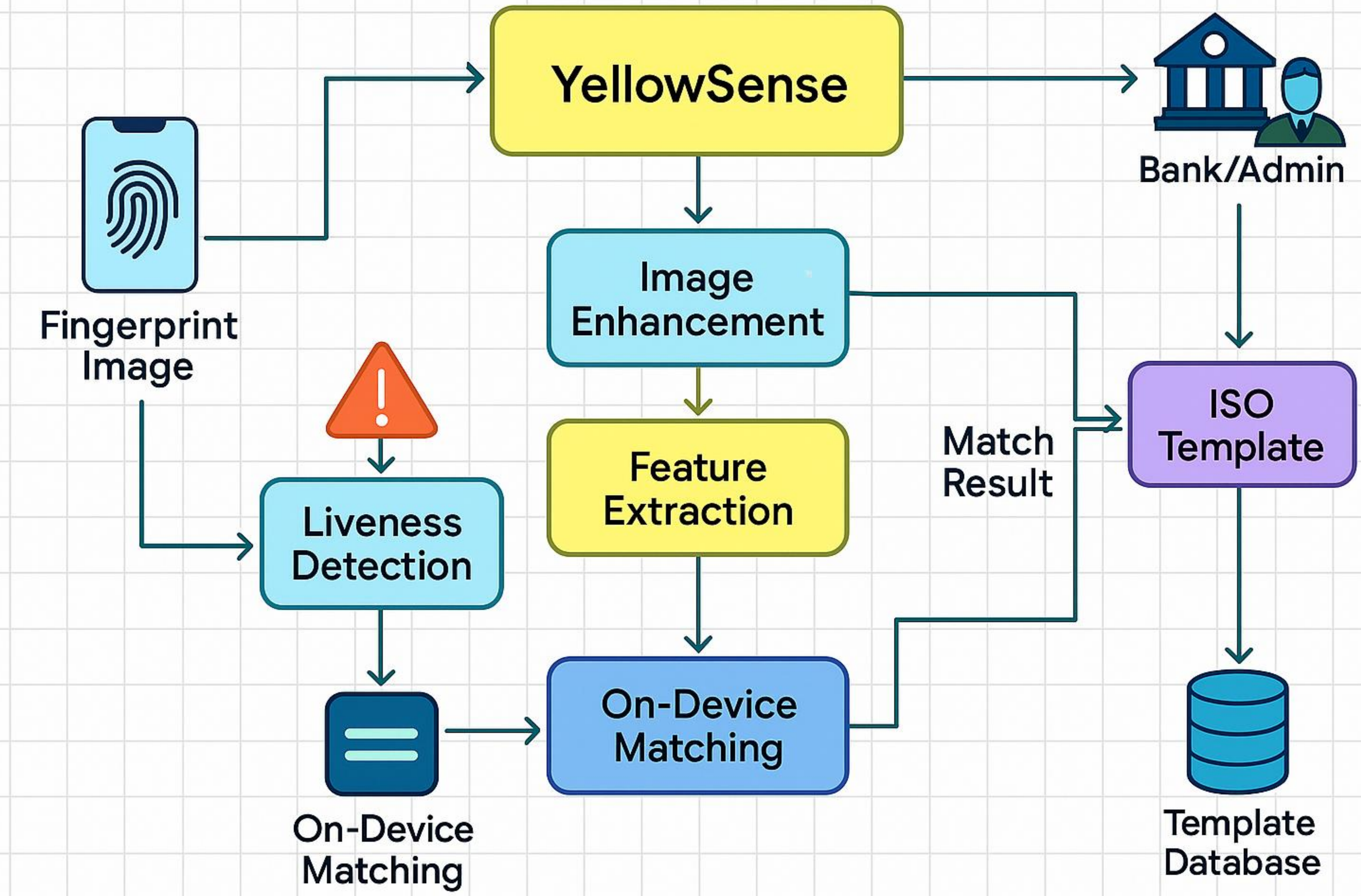
Why it fails

slow, incomplete, non-scalable, and non-compliant with privacy norms.

✓ Our edge

CCR enables *real-time, privacy-preserving, hardware-enforced* collaboration across data owners — faster, more accurate, and regulator-compliant.

our solution architecture



Our Solution/Product (contd)

01

Innovation

Confidential Computing Rooms (CCR) built on **Trusted Execution Environments (TEEs)** for *verifiable* data-in-use privacy.

02

How it works

- Data never leaves the owner → computation happens inside secure enclaves.
- Regulators/partners see only aggregated insights.

03

Unique vs others

Hardware-level trust (Intel SGX, AMD SEV) + auditability → beyond software-only clean rooms.

Target customers

- Governments (social welfare & subsidy schemes).
- Hospitals, insurers, pharma companies.
- Financial regulators, exchanges, banks.

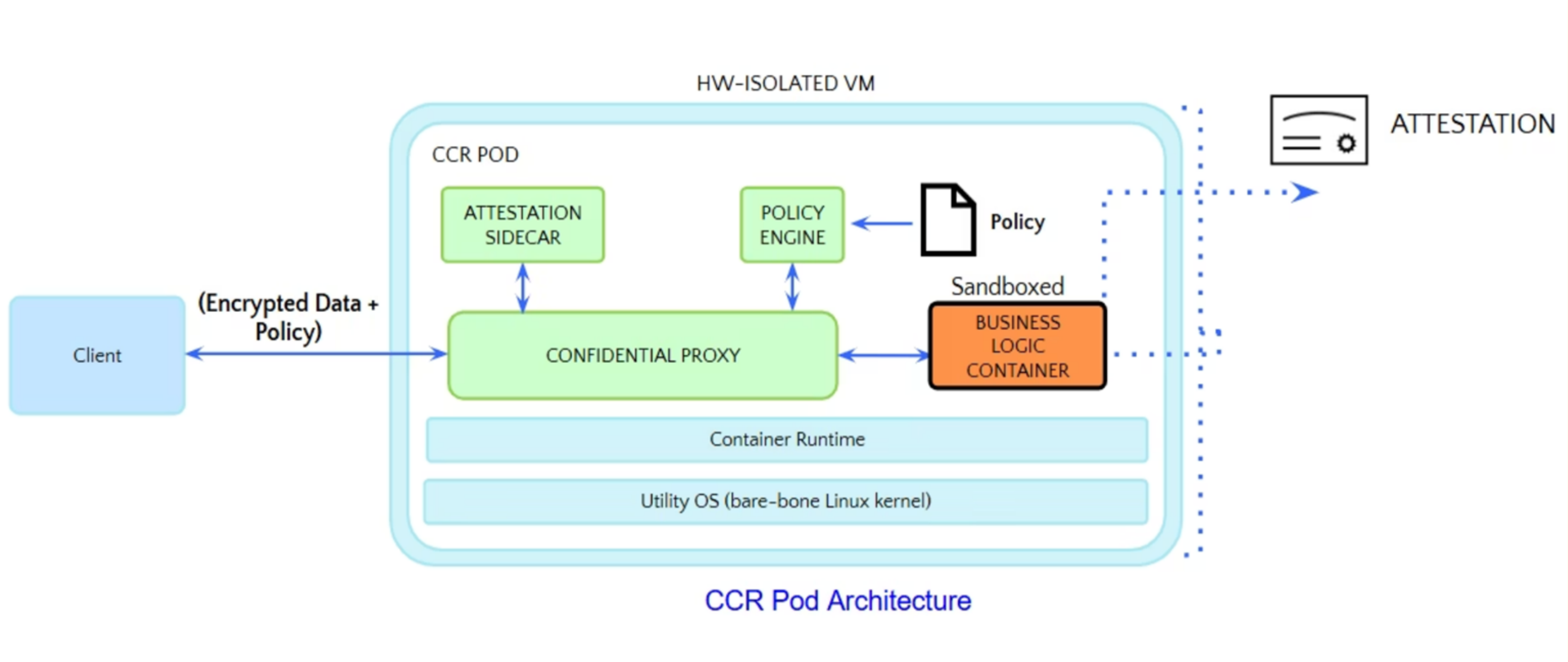
Customer need

collaborate without violating privacy or compliance.

Benefit

unlock hidden insights, reduce fraud, improve citizen outcomes.

Product Readiness Level - MVP ready - TRL 4/5



CCR Pod Architecture

Our technical architecture is meticulously designed to provide trustworthy and secure data processing services, ensuring both data integrity and confidentiality.

Secure Execution Environment

Hardware Isolation: Utilizes Confidential VMs (e.g., AMD SEV-SNP) to protect data from the infrastructure provider.

Microservice Deployment: All microservices are hosted within *CCR Pods*, a secure and controlled runtime environment.

Untrusted Logic Containment: Business logic that isn't fully trusted is executed within sandboxed containers, preventing unauthorized access or interference with critical system components.

Enhanced Security Mechanisms

Trusted Sidecar Containers: These containers perform crucial security functions such as TEE attestation, configuration verification, policy checks, and transaction history anonymization.

Data Flow Control: A trusted proxy, such as Envoy, intercepts all ingress and egress data traffic to enforce strict policy checks, ensuring only authorized data enters or leaves the system.

Trusted Execution Environments (TEEs) in Confidential Computing

Trusted Execution Environments (TEEs) are a vital component of confidential computing, providing hardware-enforced isolation to protect data and code during processing. Below are three leading hardware platforms enabling TEEs.

Intel SGX (Software Guard Extensions)

Provides hardware-isolated memory regions (enclaves) to protect sensitive code and data from privileged software attacks, enhancing application security.

ARM TrustZone

Creates a "secure world" alongside a "normal world" on ARM-based processors, offering hardware separation for critical tasks like secure boot, DRM, and cryptographic operations in mobile and IoT devices.

AMD SEV (Secure Encrypted Virtualization)

Encrypts virtual machine memory, protecting VMs from hypervisor and other VMs' access, ensuring data confidentiality and integrity in cloud environments.

Readiness

- Prototype & CCR engine already built
- Plug-and-play integration with govt data

Sustainability

- Open-source, low-cost infra
- Long-term maintainable by state IT teams
- DEPA-aligned, encrypted, auditable

Impact

- Fraud/leakage reduction in welfare schemes
- Real-time, cross-department anomaly detection
- Financial savings & increased governance trust

Efficiency

- Rapid deployment, minimal manpower
- No data duplication — federated analytics

Data Security & Compliance

- No raw data movement – secure enclaves

Socio-Economic Impact

Direct social benefits

- Prevent fraud → save investors ₹1,000+ crore/year.
- Better targeting of subsidies → reduce leakage by 15–20%.
- Faster clinical trials while protecting patient data, Reduces claim fraud (estimated ~8–10% globally) → lower premiums for citizens.

Economic benefits

- New jobs in data governance & AI model building.
- Unlock multi-billion data economy compliant with DPDP Act.

Environmental contribution

Resource efficiency via data-driven decision making (e.g., optimise health resource allocation).

Alignment with UN SDGs

- SDG 3 (Good Health & Well-Being).
- SDG 8 (Decent Work & Economic Growth).
- SDG 16 (Peace, Justice, and Strong Institutions).

Our team

Prakhar Goyal

CTO/CEO

B.Tech 2009 - **IIT Bombay** (Computer Science)

Microsoft, SAP, Amazon

Komal Goyal

MBA, Indira College

Customer Success roles at Puranik Developers

Animesh Sharma

B Tech(Final year)

IIT Patna

Kushagra

B Tech(Final year)

CMR **university**

Market Landscape

$50B

TAM (Global CCR Market)

by 2030 (CAGR ~40%)

$10B

SAM (Asia-Pacific)

privacy-first data collaboration

$500M

SOM (India)

financial + healthcare + welfare initial

Customer base

150M retail investors, 1.3B healthcare records, 800M welfare beneficiaries.

Competitors

- Clean rooms (Google Ads, Snowflake) → marketing-focused.
- Fraud vendors (Nasdaq SMARTS, NICE Actimize) → domain-specific.
- Privacy vendors (PrivaSapien) → compliance, not hardware-level CCR.

Differentiator

Hardware-backed, multi-domain CCR for India.

Revenue Model

Pricing strategy

Value-based, subscription model.

Pricing

Starting ₹5–10 lakh per CCR instance annually.

Revenue streams

- SaaS subscriptions.
- Licensing CCR framework for on-prem.
- Regulator dashboards.
- Add-on AI/ML modules (fraud detection, health analytics).

Customer LTV

₹50–75 lakh over 5 years (regulators and large enterprises typically lock-in long-term).

Roadmap: Implementation Phases (milestones)

Phase 1 (0–3 months): MVP Build & Sandbox Testing

- Develop minimal CCR prototype using open-source TEE frameworks (e.g., Intel SGX / Azure Confidential Containers).
- Ingest two small anonymised datasets (trading + social chatter).
- Run end-to-end workflow: encrypted input → enclave compute → encrypted output.
- Validate detection of simple pump-and-dump scenarios.

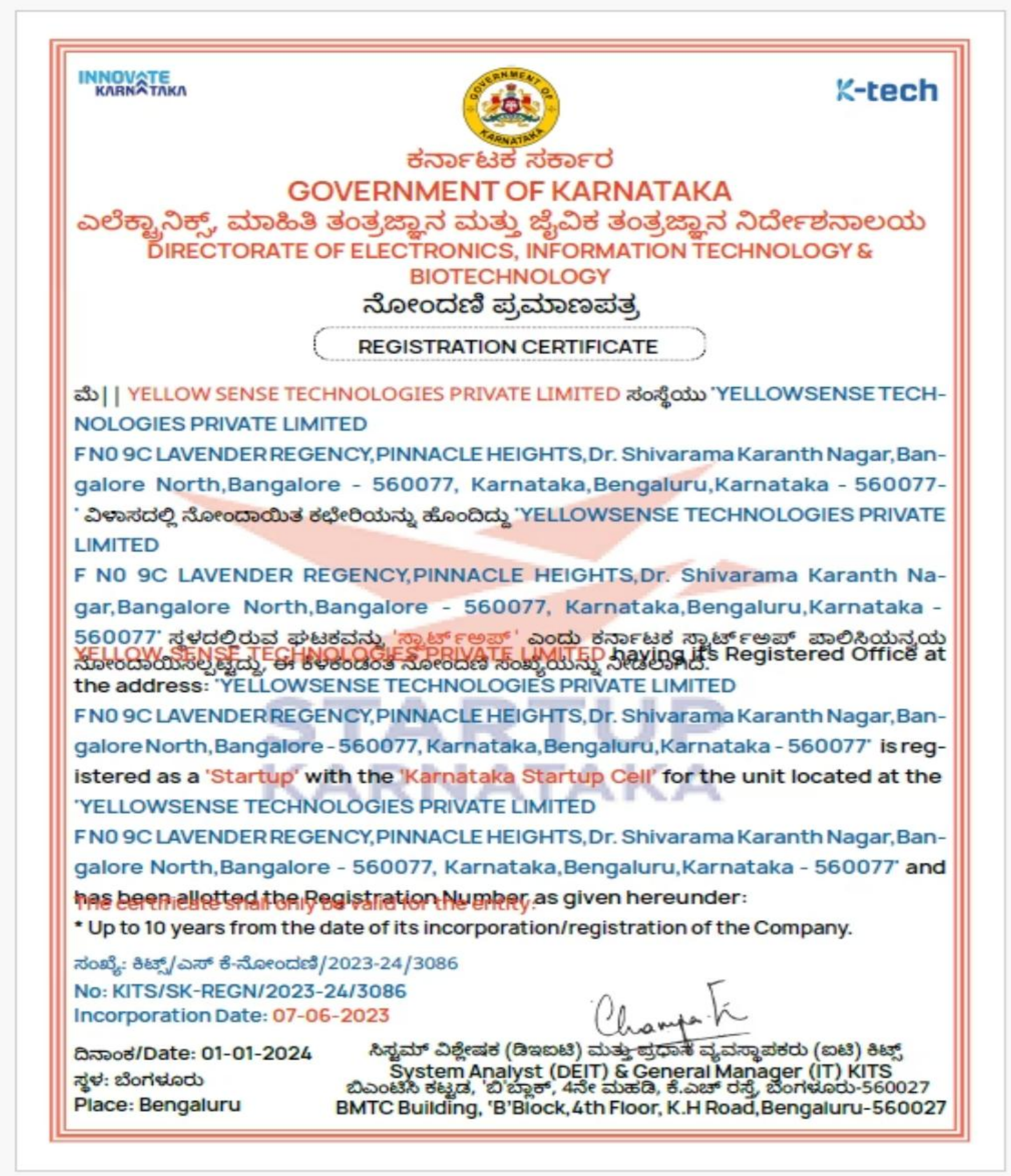
Phase 2 (3–6 months): Pilot with Test Partners

- Work with one exchange sandbox and one broker innovation lab.
- Expand detection models (volatility spikes + message surge correlation) and add a regulator-style dashboard for anomaly alerts.
- Conduct performance & privacy benchmarks (latency, scalability).

Phase 3 (6–12 months): Extended Pilot & Feedback Loop

- Onboard 2–3 additional pilot partners (bank + telco for cross-domain testing).
- Stress-test CCR under higher data volumes.
- Iterate on UX, reporting, and compliance integration (audit logs, SEBI sandbox readiness).
- Prepare for first external security certification.

We are supported by DP-IIT (Govt of India), Karnataka Govt Startup Cell



INNOVATE KARNATAKA

K-tech

ಕರ್ನಾಟಕ ಸರ್ಕಾರ

GOVERNMENT OF KARNATAKA

ಎಲೆಕ್ಟ್ರಾನಿಕ್ಸ್, ಮಾಹಿತಿ ತಂತ್ರಜ್ಞಾನ ಮತ್ತು ಜೈವಿಕ ತಂತ್ರಜ್ಞಾನ ನಿರ್ದೇಶನಾಲಯ

DIRECTORATE OF ELECTRONICS, INFORMATION TECHNOLOGY & BIOTECHNOLOGY

ನೋಂದಣಿ ಪ್ರಮಾಣಪತ್ರ

REGISTRATION CERTIFICATE

ಮೆ|| YELLOW SENSE TECHNOLOGIES PRIVATE LIMITED ಸಂಸ್ಥೆಯು 'YELLOWSENSE TECHNOLOGIES PRIVATE LIMITED
F N0 9C LAVENDER REGENCY,PINNACLE HEIGHTS,Dr. Shivarama Karanth Nagar,Bangalore North,Bangalore - 560077, Karnataka,Bengaluru,Karnataka - 560077-' ವಿಳಾಸದಲ್ಲಿ ನೋಂದಾಯಿತ ಕಛೇರಿಯನ್ನು ಹೊಂದಿದ್ದು 'YELLOWSENSE TECHNOLOGIES PRIVATE LIMITED
F N0 9C LAVENDER REGENCY,PINNACLE HEIGHTS,Dr. Shivarama Karanth Nagar,Bangalore North,Bangalore - 560077, Karnataka,Bengaluru,Karnataka - 560077' ಸ್ಥಳದಲ್ಲಿರುವ ಘಟಕವನ್ನು 'ಸ್ಟಾರ್ಟ್‌ಅಪ್' ಎಂದು ಕರ್ನಾಟಕ ಸ್ಟಾರ್ಟ್‌ಅಪ್ ಪಾಲಿಸಿಯನ್ವಯ ನೋಂದಾಯಿಸಲ್ಪಟ್ಟಿದ್ದು, ಈ ಕೆಳಕಂಡಂತೆ ನೋಂದಣಿ ಸಂಖ್ಯೆಯನ್ನು ನೀಡಲಾಗಿದೆ.

YELLOW SENSE TECHNOLOGIES PRIVATE LIMITED having it's Registered Office at the address: 'YELLOWSENSE TECHNOLOGIES PRIVATE LIMITED
F N0 9C LAVENDER REGENCY,PINNACLE HEIGHTS,Dr. Shivarama Karanth Nagar,Bangalore North,Bangalore - 560077, Karnataka,Bengaluru,Karnataka - 560077' is registered as a 'Startup' with the 'Karnataka Startup Cell' for the unit located at the 'YELLOWSENSE TECHNOLOGIES PRIVATE LIMITED
F N0 9C LAVENDER REGENCY,PINNACLE HEIGHTS,Dr. Shivarama Karanth Nagar,Bangalore North,Bangalore - 560077, Karnataka,Bengaluru,Karnataka - 560077' and has been allotted the Registration Number as given hereunder:

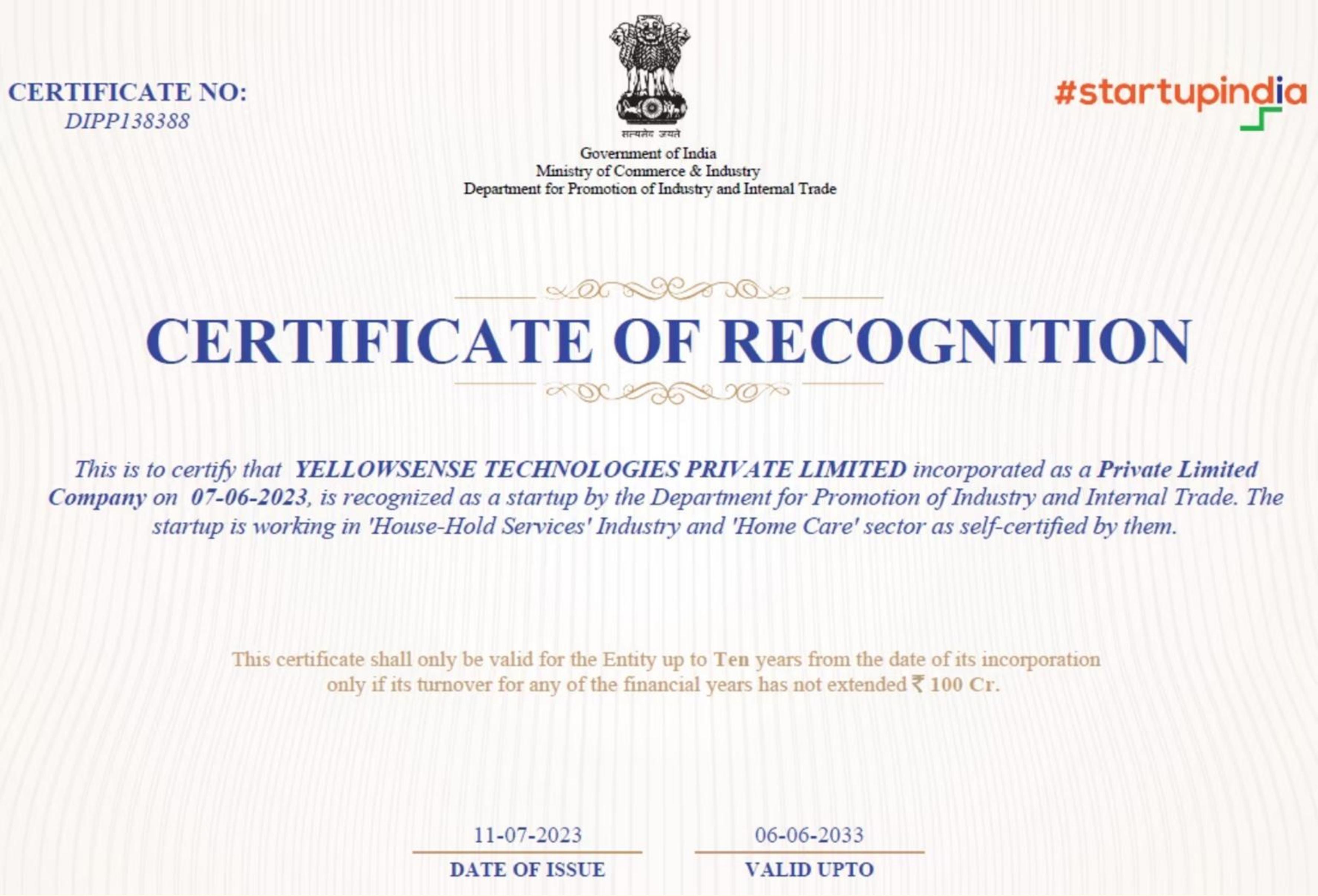
The certificate shall only be valid for the entity.

* Up to 10 years from the date of its incorporation/registration of the Company.

ಸಂಖ್ಯೆ: ಕಿಟ್ಸ್/ಎಸ್ ಕೆ-ನೋಂದಣಿ/2023-24/3086
No: KITS/SK-REGN/2023-24/3086
Incorporation Date: 07-06-2023

ದಿನಾಂಕ/Date: 01-01-2024
ಸ್ಥಳ: ಬೆಂಗಳೂರು
Place: Bengaluru

Champa K
ಸಿಸ್ಟಮ್ ವಿಶ್ಲೇಷಕ (ಡಿಇಐಟಿ) ಮತ್ತು ಪ್ರಧಾನ ವ್ಯವಸ್ಥಾಪಕರು (ಐಟಿ) ಕಿಟ್ಸ್
System Analyst (DEIT) & General Manager (IT) KITS
ಬಿಎಂಟಿಸಿ ಕಟ್ಟಡ, 'ಬಿ'ಬ್ಲಾಕ್, 4ನೇ ಮಹಡಿ, ಕೆ.ಎಚ್ ರಸ್ತೆ, ಬೆಂಗಳೂರು-560027
BMTC Building, 'B'Block,4th Floor, K.H Road,Bengaluru-560027



CERTIFICATE NO:
DIPP138388

#startupindia

सत्यमेव जयते
Government of India
Ministry of Commerce & Industry
Department for Promotion of Industry and Internal Trade

CERTIFICATE OF RECOGNITION

This is to certify that ***YELLOWSENSE TECHNOLOGIES PRIVATE LIMITED*** *incorporated as a* ***Private Limited Company*** *on* ***07-06-2023****, is recognized as a startup by the Department for Promotion of Industry and Internal Trade. The startup is working in 'House-Hold Services' Industry and 'Home Care' sector as self-certified by them.*

This certificate shall only be valid for the Entity up to **Ten** years from the date of its incorporation only if its turnover for any of the financial years has not extended ₹ **100 Cr.**

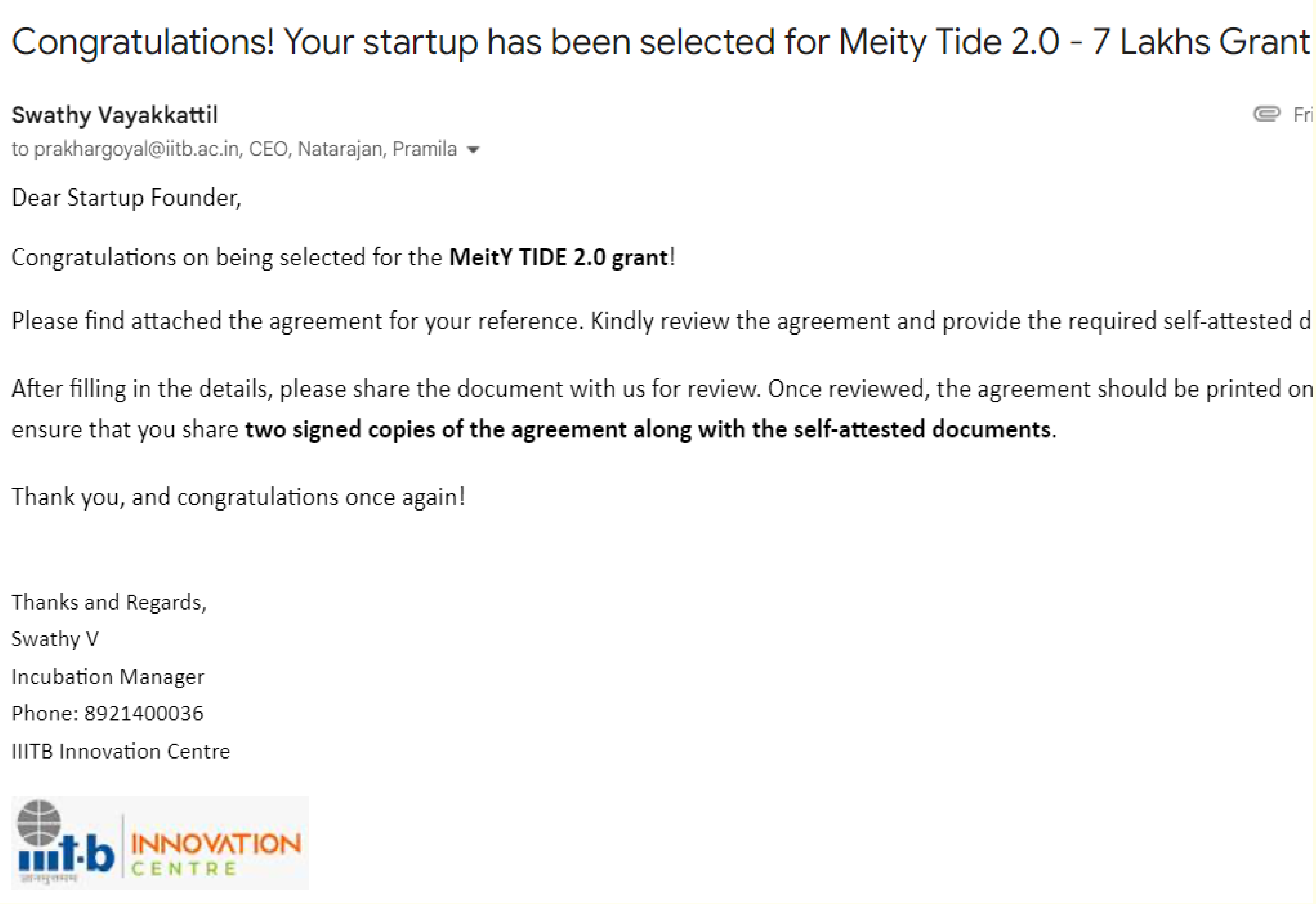
11-07-2023	06-06-2033
DATE OF ISSUE	VALID UPTO

MEITY TIDE 2.0 GRANT

received through

IIITB Innovation Center,

Bengaluru



Congratulations! Your startup has been selected for Meity Tide 2.0 - 7 Lakhs Grant

Swathy Vayakkattil Fri

to prakhargoyal@iitb.ac.in, CEO, Natarajan, Pramila

Dear Startup Founder,

Congratulations on being selected for the **MeitY TIDE 2.0 grant**!

Please find attached the agreement for your reference. Kindly review the agreement and provide the required self-attested d

After filling in the details, please share the document with us for review. Once reviewed, the agreement should be printed on ensure that you share **two signed copies of the agreement along with the self-attested documents**.

Thank you, and congratulations once again!

Thanks and Regards,
Swathy V
Incubation Manager
Phone: 8921400036
IIITB Innovation Centre

Incubation details

nasscom startups

iiit-b INNOVATION CENTRE

ज्ञानमुत्तमम्

Physically incubated

STPINEXT INITIATIVES

Awards

Supported by all leading cloud providers

Microsoft Azure

Google Cloud

aws

Awards & Recognition

We are proud to have been selected among the Top 40 Product Launches at the highly esteemed Bengaluru Tech Summit. This recognition underscores our commitment to innovation and the significant impact our solutions are making in the technology landscape.