CYSE 587

ANONYMOUS AUTHENTICATION FOR UTM ACCESS

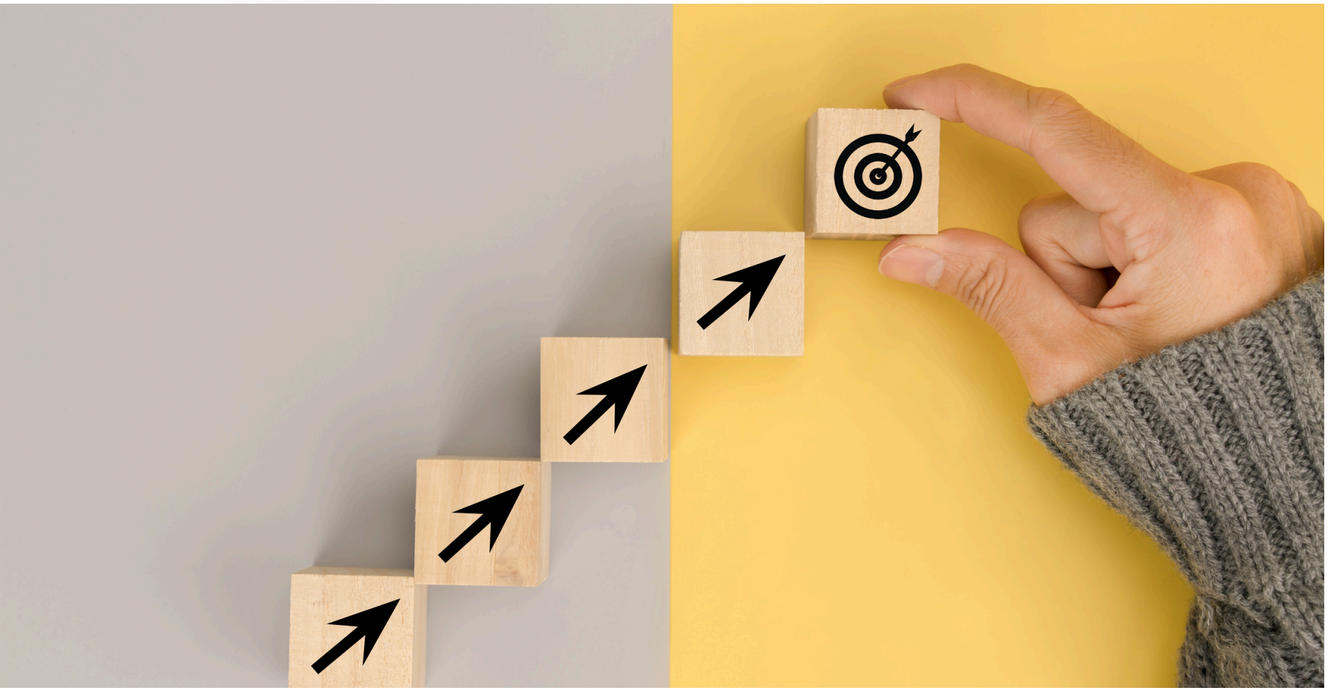
Group B

WHAT IS UTM / U-SPACE?

UTM is a digital ecosystem that manages low-altitude UAV operations by providing:

- Decentralized traffic management for drones
- Real-time coordination between UAVs, operators, USS providers, and regulators
- Integration support for autonomous and high-density drone operations
- Safety and airspace compliance at scale

UTM OPERATIONAL GOALS



- Safety: prevent mid-air conflicts and unauthorized operations
- Accountability: ensure only authorized operators access UTM
- Security: protect against spoofing, impersonation, replay
- Performance: support thousands of simultaneous UAV flights
- Scalability: accommodate national-level drone ecosystems

UTM OPERATIONAL PHASES

1- Registration
- Operator/UAV identity validation

2- Planning
- Flight intent submission & approval

3- Tactical
- Real-time auth + Remote ID broadcasts

4- Oversight / Strategic
- Logging, auditing, compliance enforcement

US VS EU REMOTE ID APPROACHES

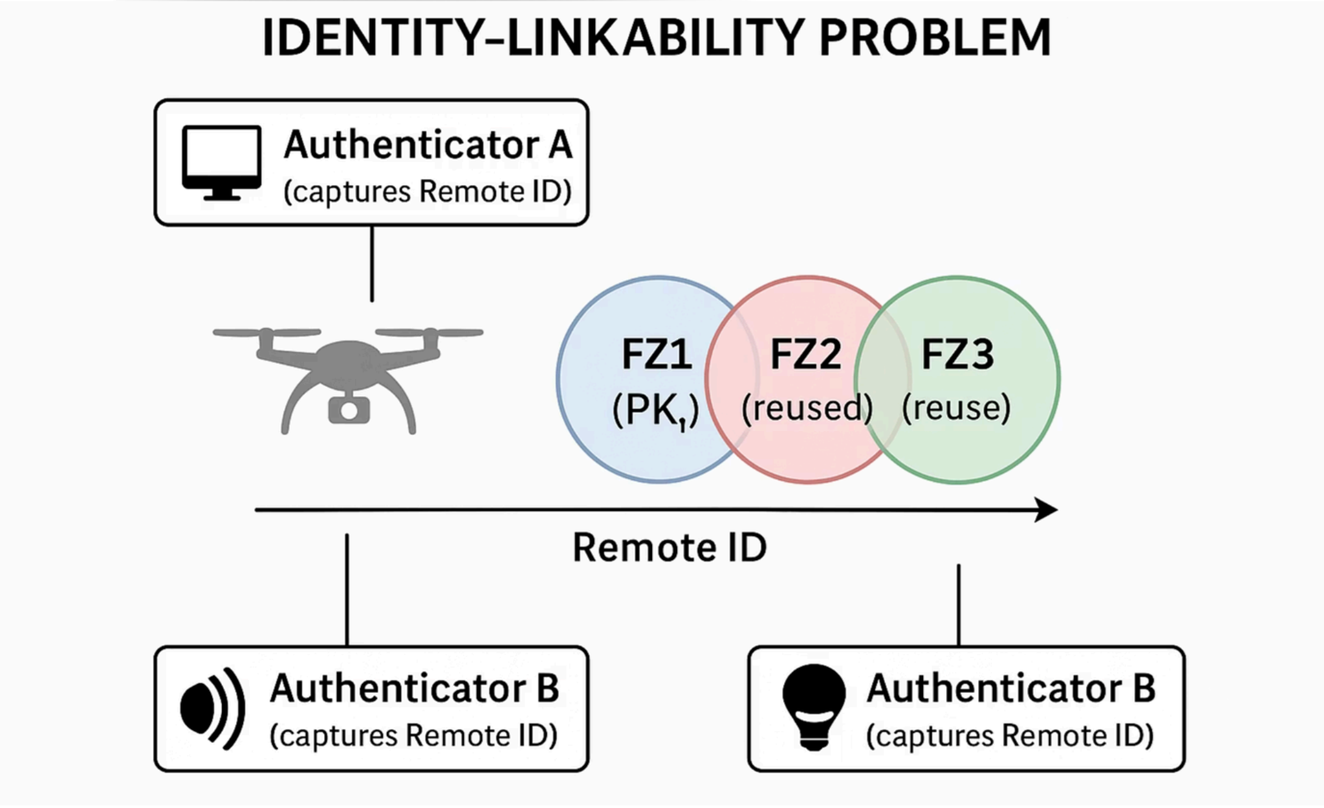
UNITED STATES (FAA)

- Persistent Remote ID broadcast
- Identity is public & linkable

EUROPEAN UNION (U-SPACE / EASA)

- Emphasizes privacy by design
- Limits unnecessary disclosure of operator identity

THE IDENTITY-LINKABILITY PROBLEM

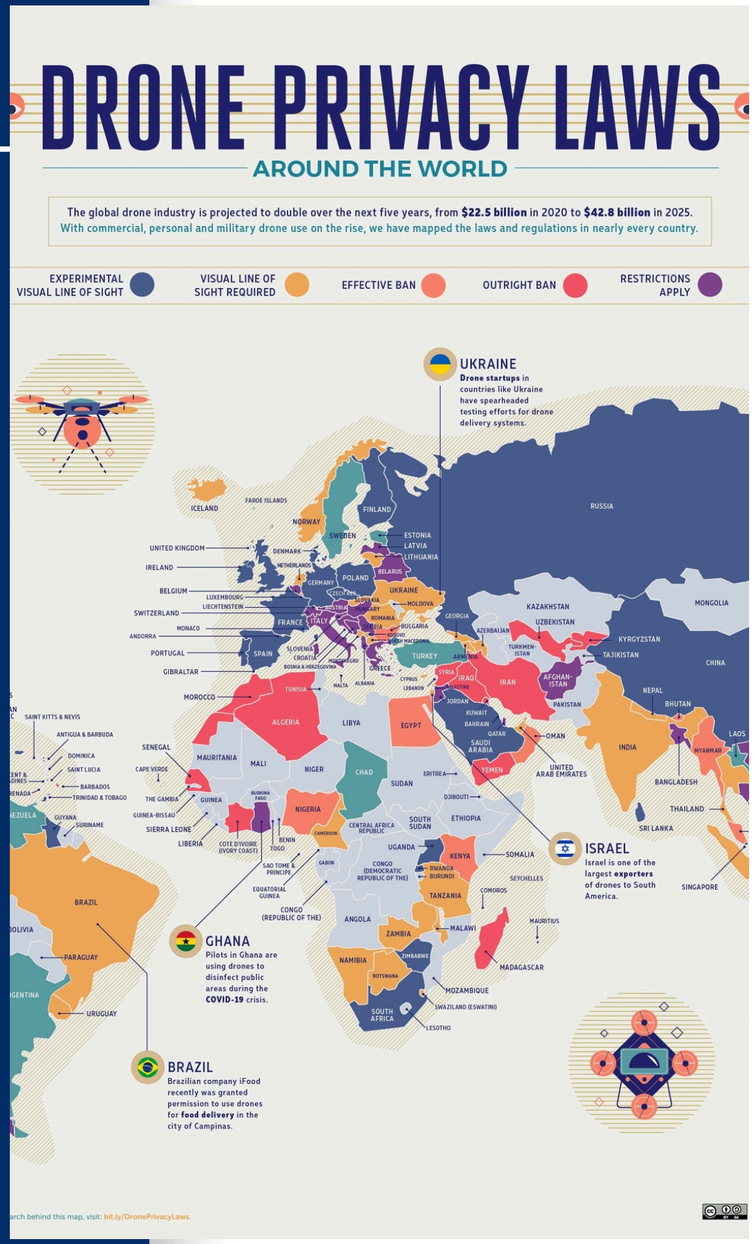


- Remote ID often broadcasts a single persistent identifier
- Multiple authenticators can correlate broadcasts across zones
- Enables reconstruction of flight paths
- Exposes operator identity, home base, client sites
- Creates commercial, privacy, and safety risk

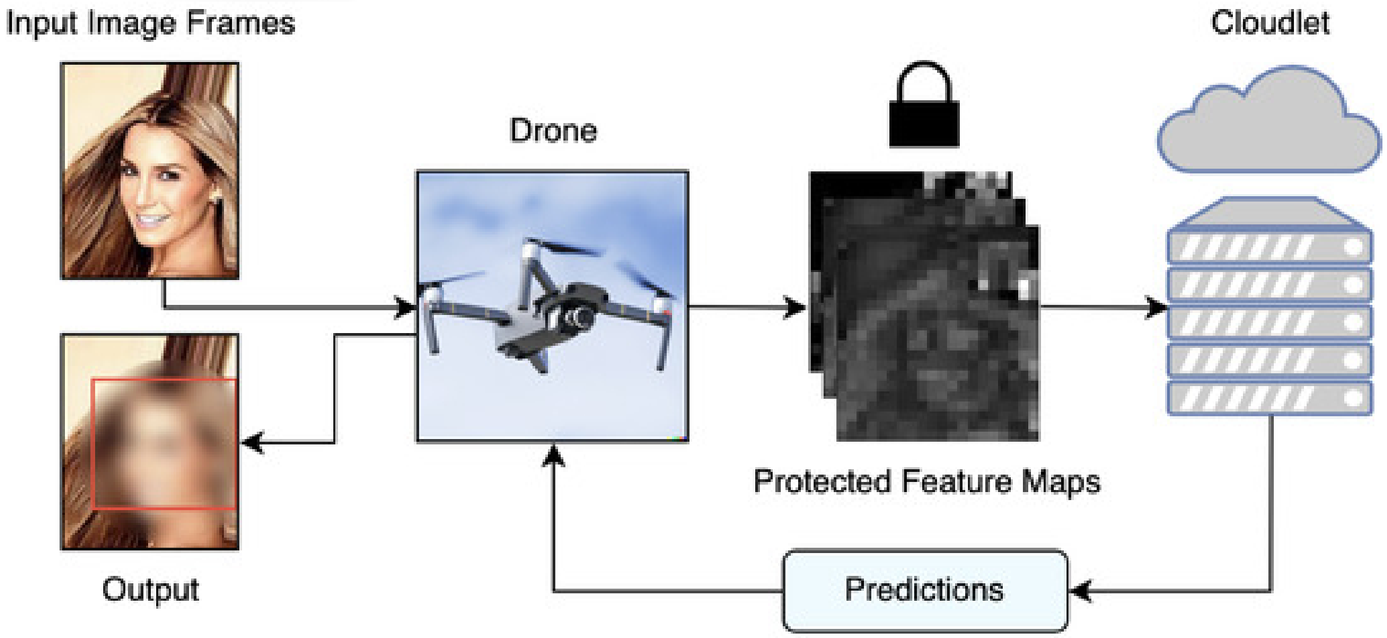
WHY IDENTITY-LINKABILITY MATTERS

Operators face:

- Loss of operational confidentiality
- Exposure to competitors
- Physical or cyber targeting
- Reduced willingness to adopt UTM



PROBLEM STATEMENT



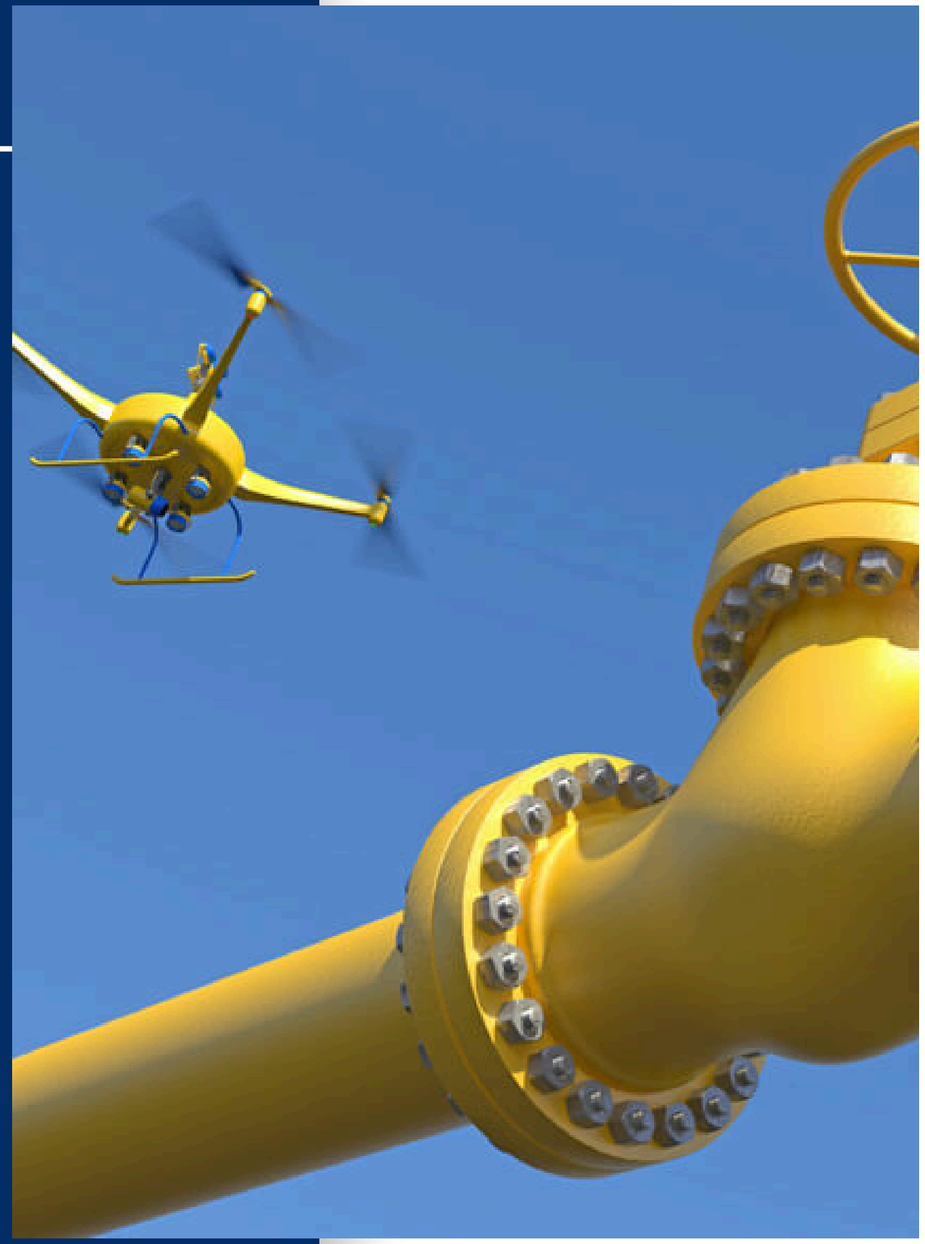
- Current Remote ID + UTM authentication mechanisms:
- Expose operator identity during tactical operations
- Enable cross-flight linkability
- Create privacy and trust barriers
- Limit UTM adoption and scalability

DRONES ARE BECOMING CRITICAL INFRASTRUCTURE

UTM must support:

- Logistics & delivery networks
- Agriculture automation
- Industrial inspection
- Emergency response & public safety
- National-scale autonomous operations

Growing scale → higher stakes for privacy + security.



IDENTITY-BASED UTM = PRIVACY PROBLEM

AUTHENTICATION TODAY TIES REAL-WORLD OPERATOR IDENTITY TO:

- Flight paths
- Mission frequency
- Operational zones
- Client locations

LEADING TO:

- Commercial intelligence leakage
- Safety risks
- Target profiling

PRIVACY RISK SLOWS ADOPTION

Operators hesitate because:

- Their operations are exposed
- Competitors can observe patterns
- Sensitive missions become traceable
- Regulatory burden increases

UTM adoption drops without strong privacy guarantees.

STAKEHOLDER MAPPING

Primary Actors

- UAV Operator – Requests credentials, flies missions, must protect mission privacy.
- UAV / On-board Module – Stores pseudonyms, signs telemetry.
- UTM Service Provider – Verifies credentials, enforces policies.

Credential Ecosystem

- Enrollment & Identity Authority (EIA) – Performs one-time civil identity verification.
- Pseudonym Certificate Authority (PCA) – Issues short-lived anonymous credentials.
- Verifier Nodes – Validate signatures and detect replay.

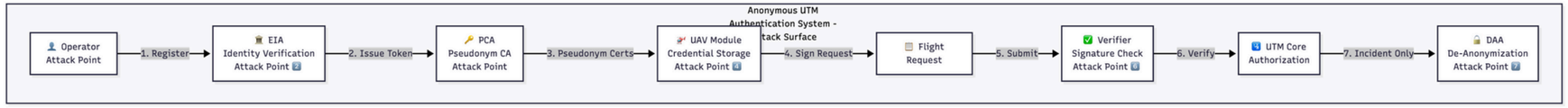
Governance / External

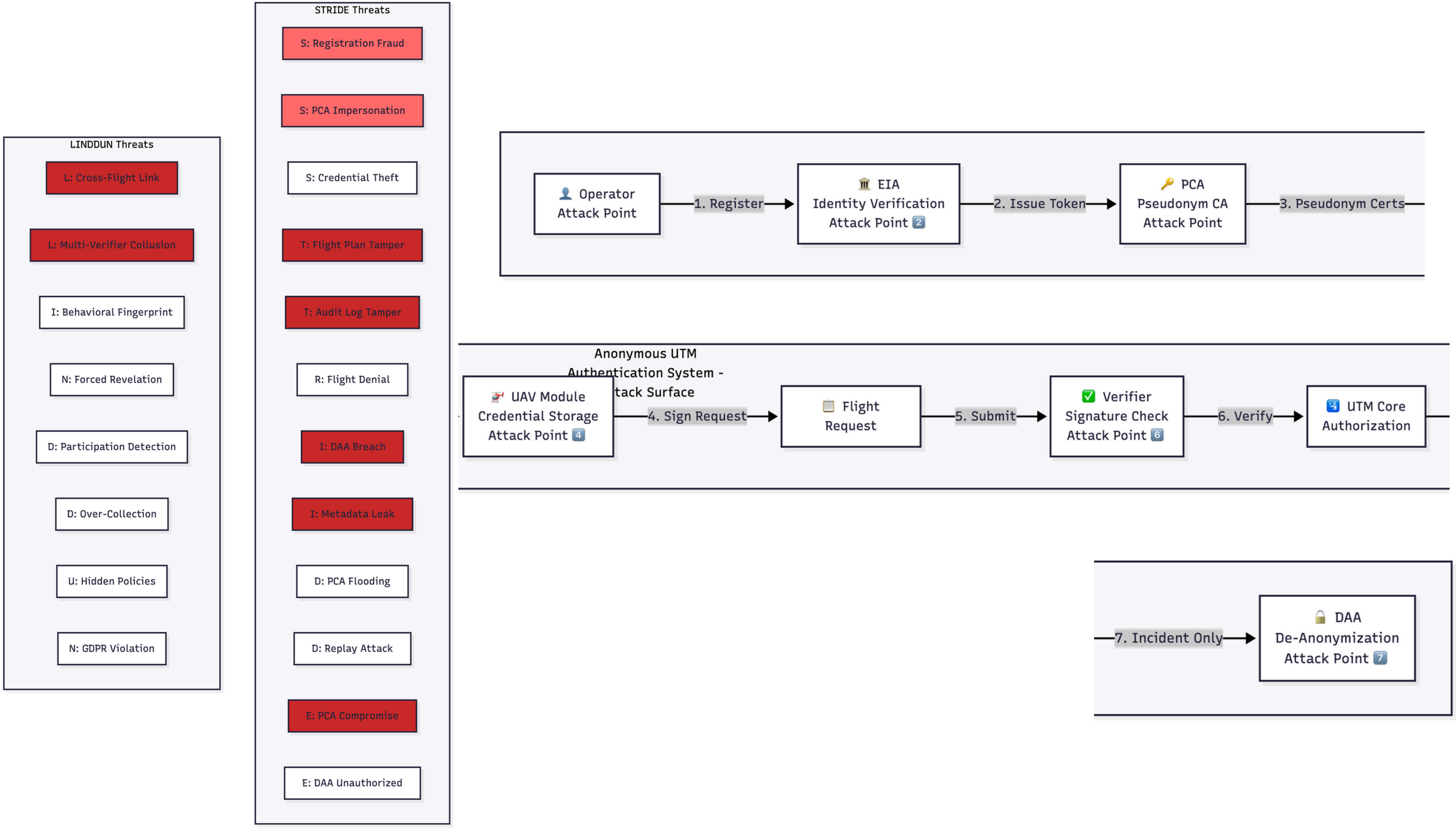
- Regulators (FAA / national aviation) – Require accountability and Remote ID compliance.
- Public / Bystanders – Expect privacy-preserving operations.
- Adversaries – Attempt linkability, spoofing, replay, or metadata extraction.

Why It Matters

- Stakeholders define the requirements, attack surfaces, and the trust model.

THREAT MODEL (STRIDE + LINDDUN)



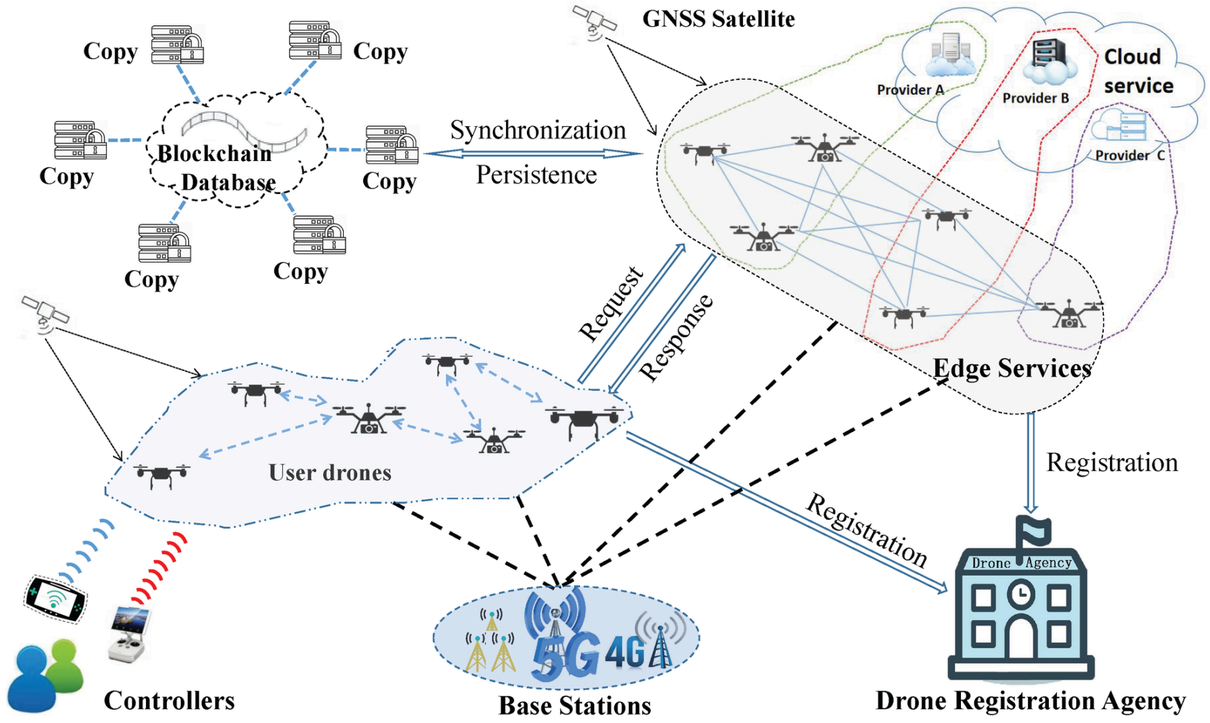

LINDDUN Threats
L: Cross-Flight Link
L: Multi-Verifier Collusion
I: Behavioral Fingerprint
N: Forced Revelation
D: Participation Detection
D: Over-Collection
U: Hidden Policies
N: GDPR Violation
STRIDE Threats
S: Registration Fraud
S: PCA Impersonation
S: Credential Theft
T: Flight Plan Tamper
T: Audit Log Tamper
R: Flight Denial
I: DAA Breach
I: Metadata Leak
D: PCA Flooding
D: Replay Attack
E: PCA Compromise
E: DAA Unauthorized
Operator Attack Point
1. Register
EIA Identity Verification Attack Point 2
2. Issue Token
PCA Pseudonym CA Attack Point
3. Pseudonym Certs
Anonymous UTM
tack Surface
UAV Module Credential Storage Attack Point 4
4. Sign Request
Flight Request
5. Submit
Verifier Signature Check Attack Point 6
6. Verify
UTM Core Authorization
7. Incident Only
DAA De-Anonymization Attack Point 7

UNLOCKING UTM WITH ANONYMOUS AUTHENTICATION

Our solution introduces an authentication layer that:

- Proves authorization without revealing civil identity
- Protects flight patterns from linkability
- Supports controlled identity reveal (DAA) only during incidents
- Aligns with privacy-by-design initiatives
- Improves trust for operators & regulators

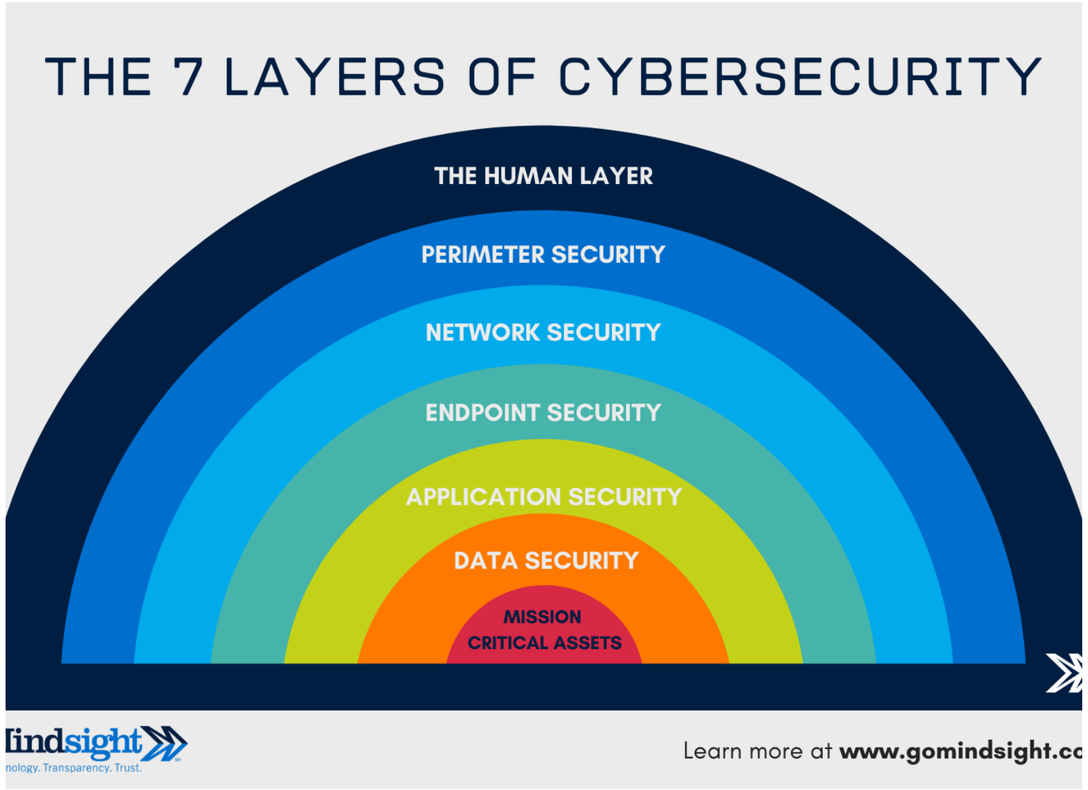
SOLUTION OVERVIEW



A privacy-preserving authentication system using:

- Short-lived pseudonyms
- Anonymous digital credentials
- Verifier that checks authorization, not identity
- Legal-only de-anonymization path

KEY SECURITY PATTERNS USED

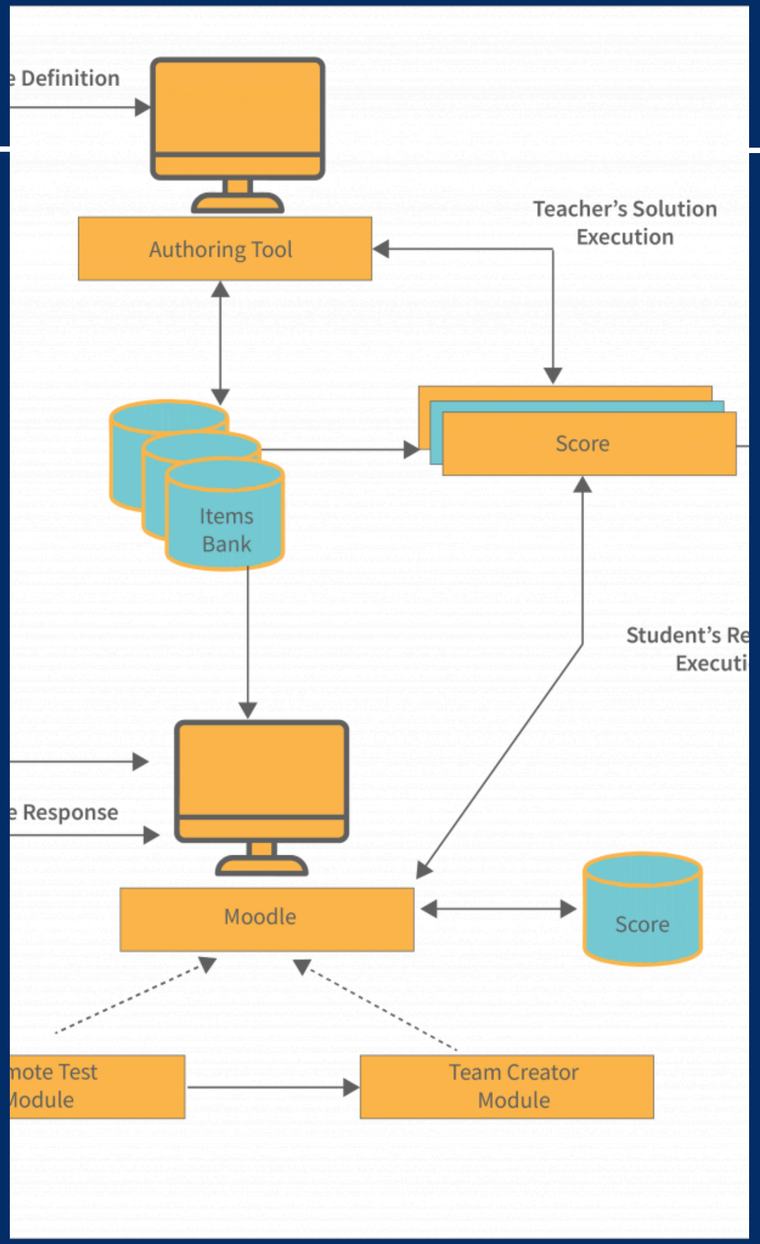


- Credential Authority Pattern (PCA)
- Enrollment & Identity Authority (EIA)
- Gatekeeper / Broker Pattern (UTM Core)
- Secure Audit Log Pattern (DAA)
- Secure Channel Pattern (TLS)

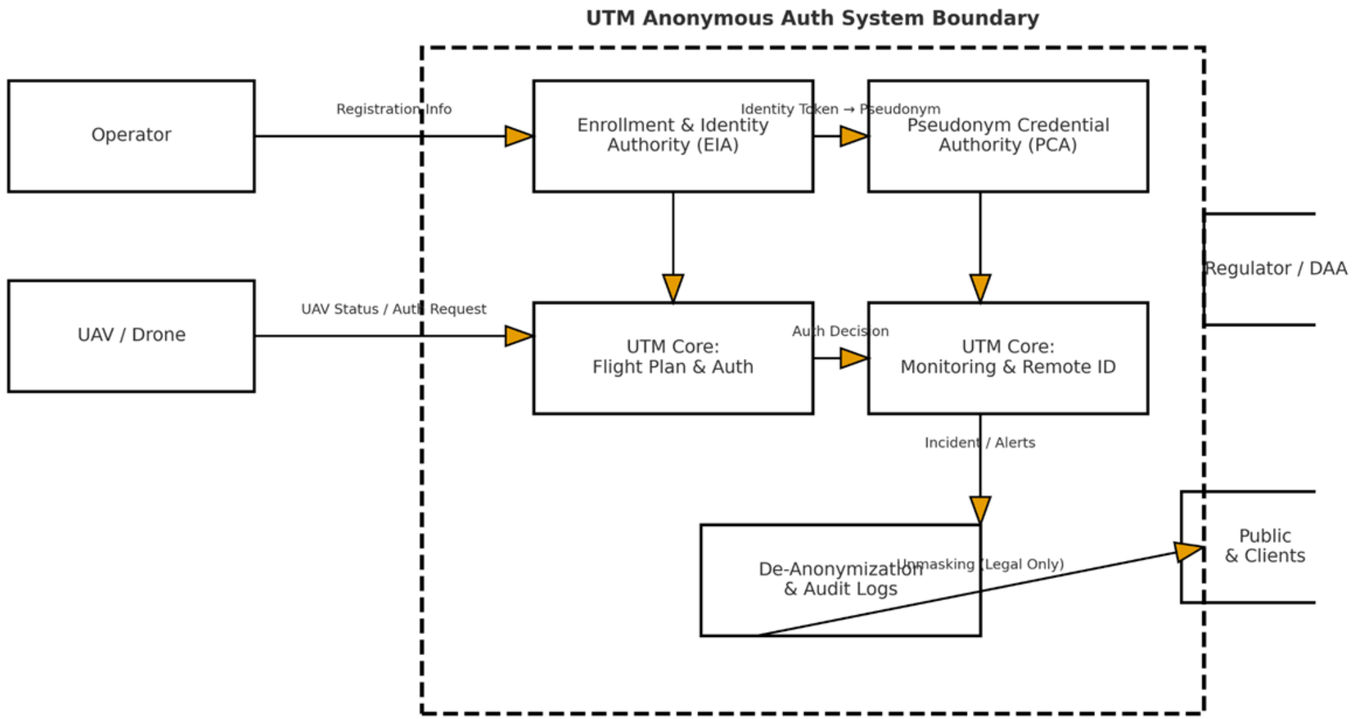
These patterns ensure identity protection + operational safety.

COMPONENT OVERVIEW

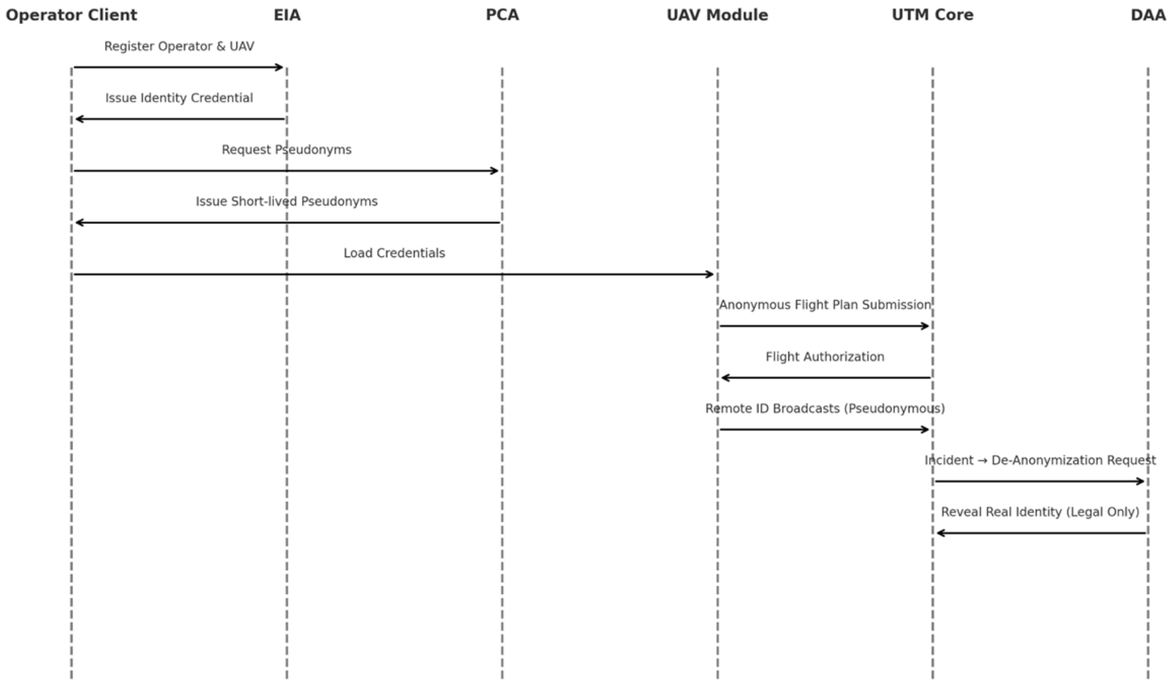
- Operator Client: requests pseudonyms
- EIA: verifies civil identity once
- PCA: issues anonymous short-lived credentials
- UAV Module: stores pseudonymous keys
- UTM Core: verifies anonymous requests
- DAA: handles controlled identity reveal



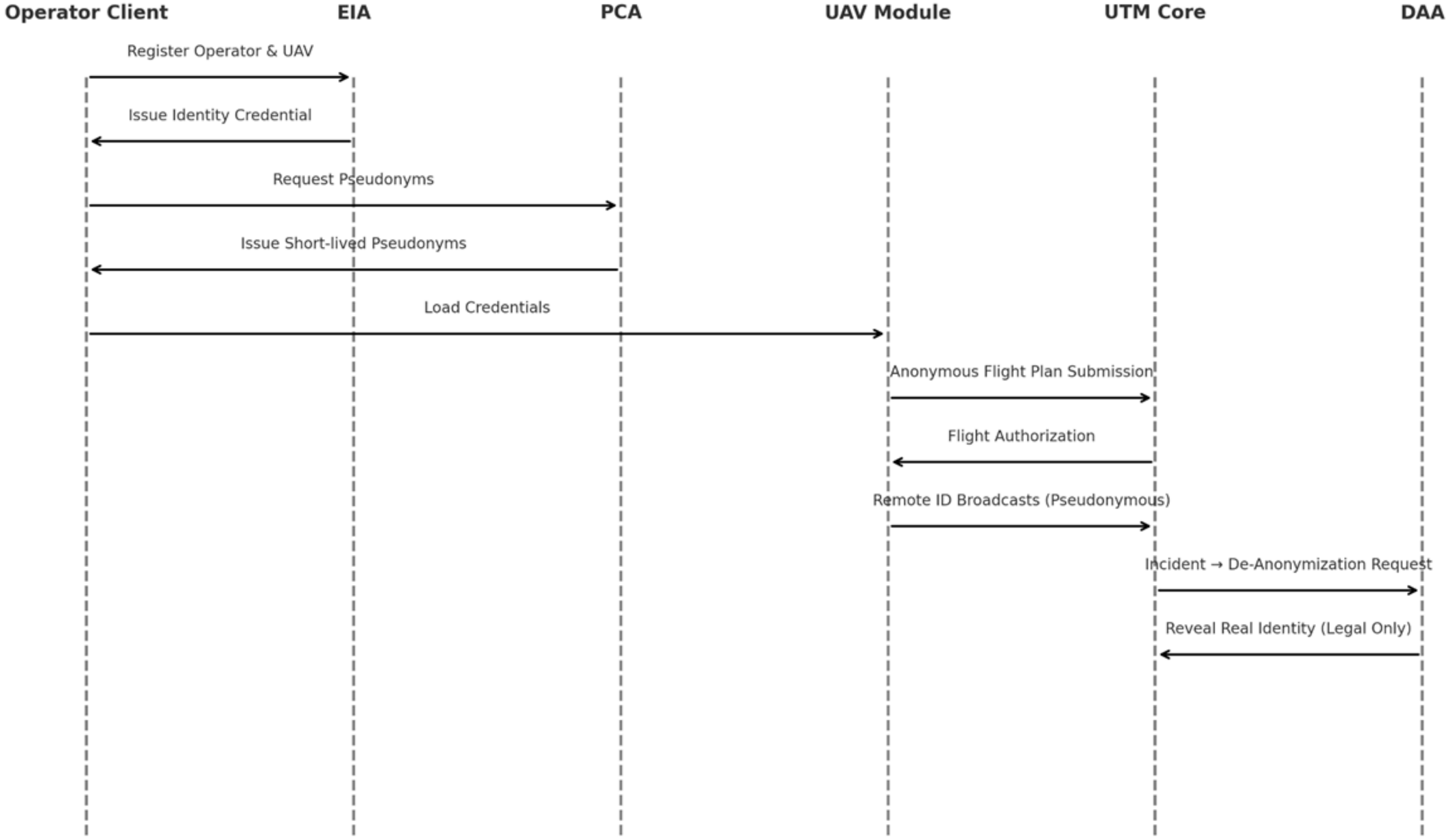
HIGH-LEVEL ARCHITECTURE



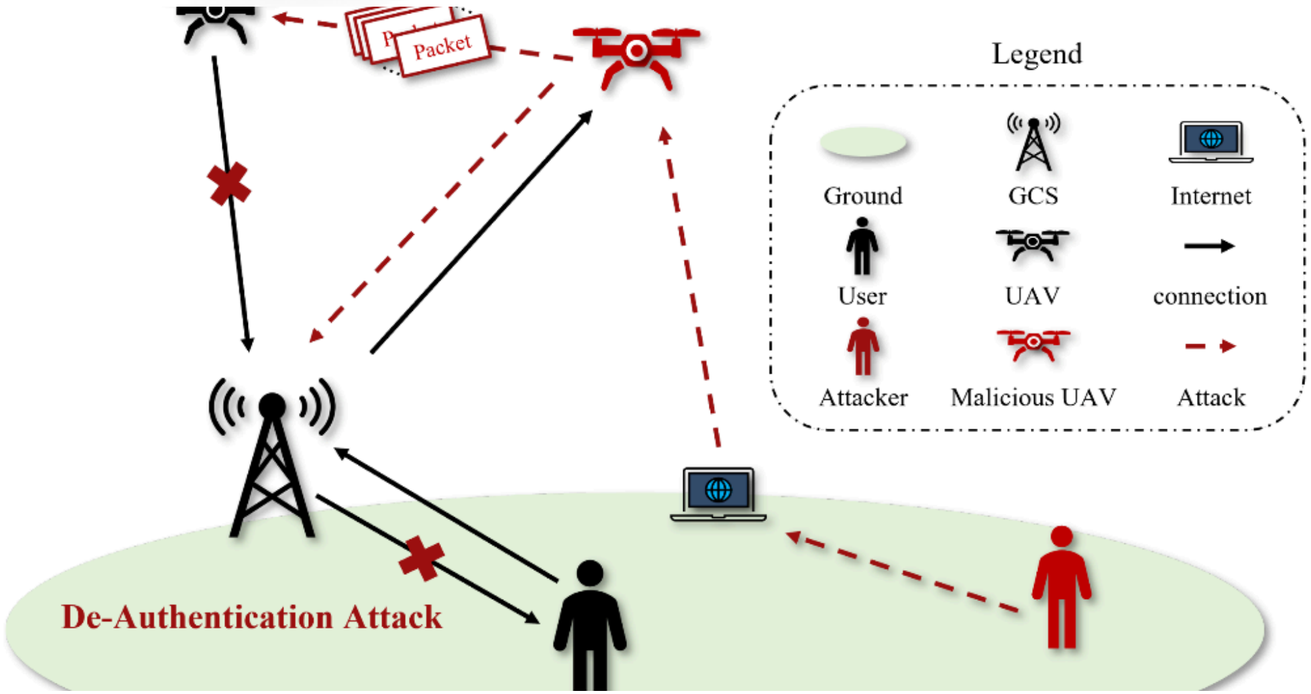
DETAILED SEQUENCE SUMMARY



- Operator registers with EIA
- PCA issues short-lived anonymous credentials
- UAV loads pseudonyms securely
- UAV submits anonymous authorization request
- UTM verifies without identity
- UTM authorizes or denies
- DAA reveals identity only with legal trigger


Operator Client
EIA
PCA
UAV Module
UTM Core
DAA
Register Operator & UAV
Issue Identity Credential
Request Pseudonyms
Issue Short-lived Pseudonyms
Load Credentials
Anonymous Flight Plan Submission
Flight Authorization
Remote ID Broadcasts (Pseudonymous)
Incident → De-Anonymization Request
Reveal Real Identity (Legal Only)

ATTACK SURFACE OVERVIEW



Attackers can influence:

- UAV ↔ UTM wireless channel
- Credential issuance workflow
- UTM Verifier infrastructure
- Logging & audit paths
- Multi-UTM federation

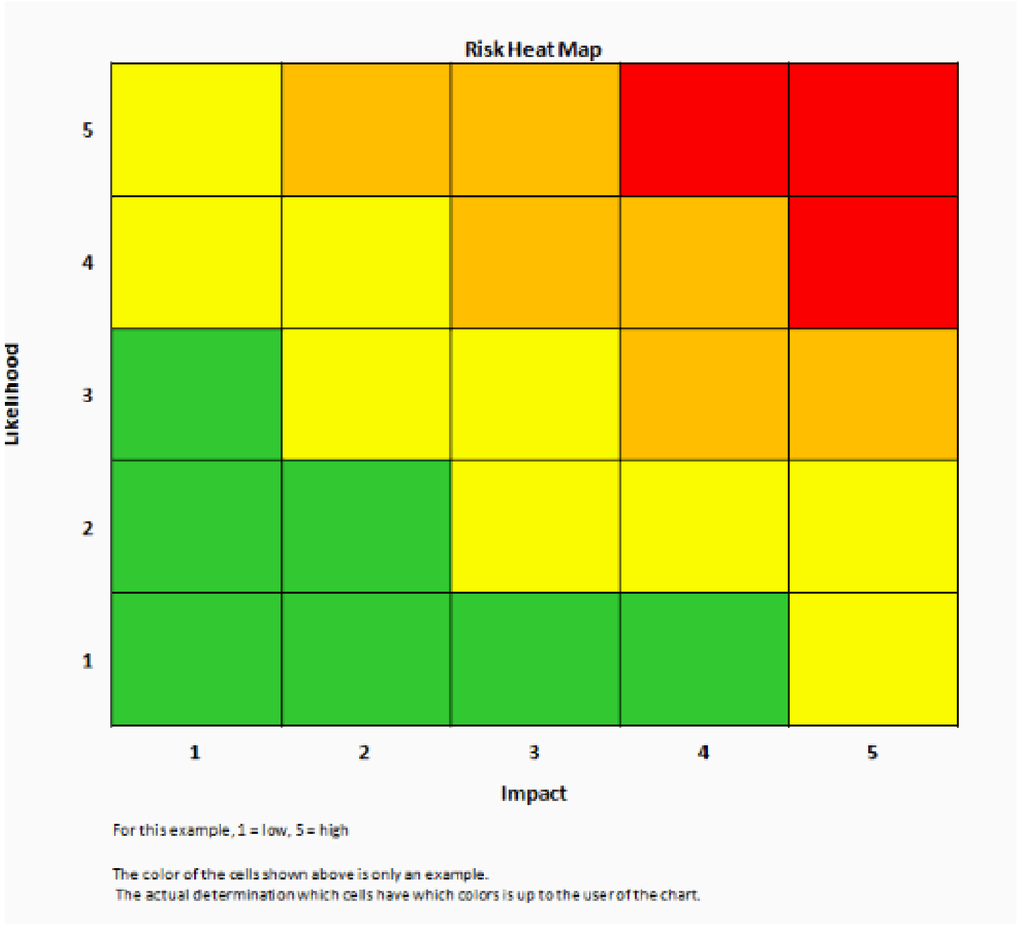
These surfaces are the basis for our threat analysis.

CRITICAL THREATS IDENTIFIED

- Replay Attacks
- Linkability Attacks
- Credential Authority Compromise
- Verifier Collusion
- Audit Log Tampering

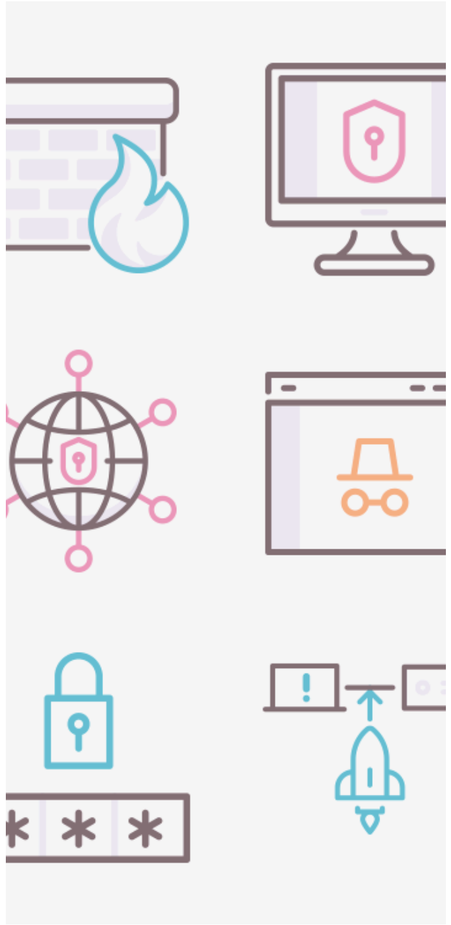
Security + privacy issues combined.

QUANTITATIVE RISK MATRIX



- Linkability: Critical (High impact, High likelihood)
- Replay: High (Medium likelihood, High impact)
- PCA compromise: High
- Verifier collusion: High
- Log tampering: Medium-High

SECURITY & PRIVACY REQUIREMENTS



SECURITY REQUIREMENTS

- S-1: Mutual authentication
- S-2: Replay resistance
- S-3: Controlled credential issuance

PRIVACY REQUIREMENTS

- P-1: Unlinkability
- P-2: Metadata minimization
- P-3: Controlled deanonymization

INTEGRITY & ACCOUNTABILITY

- I-1: Key isolation
- A-1: Verifier integrity
- N-1: Immutable logs

REQUIREMENTS TRACEABILITY MATRIX

Requirement	**Threat Addressed**	Category
R1 – Mutual Authentication	Spoofing, DoS	Security
R2 – Replay Resistance	Replay Attacks (STRIDE “R”)	Security
R3 – Unlinkability	Linkability, Identifiability	Privacy
R4 – Metadata Minimization	Detectability, Profiling	Privacy
R5 – Controlled De-anonymization (DAA)	Accountability, Non-repudiation	Integrity
R6 – Log Integrity	Tampering (STRIDE “T”)	Accountability
R7 – Key Isolation	PCA compromise / Privilege escalation	Security

ARCHITECTURE VS REQUIREMENTS

Unlinkability (R3)

- PCA issues short-lived pseudonym certificates
- UAV rotates pseudonyms frequently

Mutual Authentication (R1)

- TLS + signed credentials between UAV ↔ UTM

Replay Protection (R2)

- Nonce + timestamp validation in verifier
- Demo replay detection module

Controlled De-anonymization (R5)

- DAA component holds identity escrow keys
- Reveal only triggered by legal authority

Metadata Minimization (R4)

- No civil identity sent over UTM
- Only anonymous signatures + flight data

Log Integrity (R6)

- Append-only logs
- Hash-chained audit trails (Secure Audit Log Pattern)

KEY TRADE-OFFS

- Privacy vs Accountability
- Performance vs Cryptographic Security
- Scalability vs System Complexity
- Public Trust vs Operational Overhead
- Our architecture balances all four.

DEMO OVERVIEW

We implemented:

- Credential generation
- Anonymous signature creation
- UTM verification workflow
- Replay attack detection
- Linkability probability simulation

Shows feasibility & impact.

DEMO

Anonymous Authentication for UTM

Technical Demonstration Notebook

Prepared by: Group B
Course: CYSE 587 — Deliverable 3
Demo: Anonymous Authentication for UTM

[16]:
```
# ============================================================
# REQUIRED IMPORTS
# ============================================================

import hashlib
import time
import random
import matplotlib.pyplot as plt
from datetime import datetime
import hmac
import os

print("All modules imported successfully!")
```

```
All modules imported successfully!
```

[7]:
```
# --------------------------------
# STEP 1: PSEUDONYM GENERATION
# --------------------------------

def generate_pseudonym():
    """Generate a short-lived anonymous pseudonym using randomness + timestamp."""
    raw = str(random.random()) + str(time.time())
    return hashlib.sha256(raw.encode()).hexdigest()[:16]   # 16-char pseudonym
```

VALIDATION SCENARIOS

TACTICAL AUTHENTICATION VALIDATION

Replay prevention, signature checking

FEDERATED UTM PRIVACY STRESS TEST

Unlinkability under multiple verifiers

REMOTE ID PSEUDONYM INTEGRITY TEST

No cross-flight correlation

KEY CONTRIBUTIONS

- Privacy-first UTM authentication
- Anonymous + accountable design
- Strong demo evidence
- Scalable, regulator-friendly architecture
- Solves the identity-linkability problem

FUTURE WORK

- Multi-PCA deployment
- Formal verification of unlinkability
- Integration with LAANC and Remote ID ecosystems
- Hardware-backed pseudonym attestation

THE END