

# CASE STUDY BIOMETRICS

## Operational Situation

High-volume border checkpoints, authorities must rapidly process individuals while maintaining national security, humanitarian compliance, and operational efficiency. Traditional methods rely on paper documentation, centralized databases, or fragile network connectivity creating risk during surges, remote deployments, or infrastructure disruption.

## Operational Challenges

A multi-agency border checkpoint experiences a surge of migrant crossings. Processing teams must:

- Verify identity
- Determine if individuals are on watchlists
- Detect known threats or prior deportees
- Maintain processing speed
- Operate in austere conditions with unreliable connectivity

The checkpoint operates with:

- P25 LMR for tactical voice
- LTE for data backhaul
- SATCOM for redundancy

## Solutions Implemented

Kenwood Kairos repeater

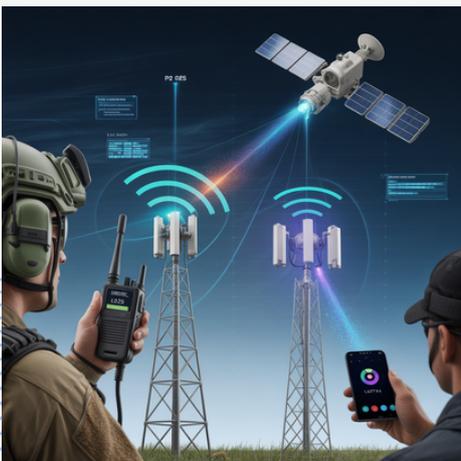
Kenwood VP8000

Starlink

Rugged Android Phones running:

- ESChat
- Identity Warrior

Interop Box



## System Architecture

1. Individual arrives at processing station
2. Agent uses Android device running:
  - INSITE for biometric capture & documentation
  - Identity Warrior for watchlist matching & ACL management
3. Multi-modal capture performed:
  - Face
  - Fingerprints (contact or contactless)
  - Iris (if required)
4. Software checks against:
  - Local watchlists (unlimited size)
  - Customer-defined databases
  - DoD ABIS (if network available)
5. Match/no-match response returned
  - If match:
    - TAK spot report generated
    - Alert transmitted across P25/LTE/SATCOM network
    - Command center notified
6. If no match:
  - Individual enrolled
  - ID badge optionally generated
  - Record synchronized peer-to-peer

## Results and Impact

- Real-time biometric watchlist screening
- Offline capability during network outages
- Rapid throughput
- Reduced false identity claims
- Secure communications backhaul over P25/LTE/SATCOM