TSA Biometrics Landscape

Enterprise Architecture Analysis

Ramana Kasibhotla, TSA

May 15, 2018

Transportation Security Administration

Overview

Biometrics Study Introduction

- The Enterprise Architecture Division (EAD) set out to identify all TSA systems/services that leverage biometric data
- Purpose of the study:
  - Current State Architecture
    - » Analyzes the structure of the current biometric landscape and identifies alignment of data, technology/capabilities, and business processes
    - » Captures specific information to answer:
      - What information is currently being captured
      - Where is the information being captured, stored, and used
      - How is the information being utilized and captured
      - Does the data interface, or is it shared, with other systems/services or offices
  - Future State Recommendations & Strategy
    - » Analysis that captures collaboration and consolidation opportunities between systems/services, offices, and agencies and describes their interactions
    - » Presents a strategy/recommendations to achieve a Future State, including:
      - Recommendations on how to handle current biometric information
      - How to improve/enhance TSA mission and capabilities using biometrics
      - Implementation of other biometric standards and best practices
      - Guidance on how TSA can better adapt to current DHS biometrics landscape and expected future capabilities
  - Future Biometric Technology & Capabilities
    - » Recommendations for new technology/capabilities that could be implemented at TSA

Current State Architecture

Approach for Gathering Information

- Enterprise Architecture Team provided an initial list of systems and programs that leverage biometric information to start the study with
- Extensive research was done internally at TSA (iShare, EAIR, CollabNet, etc.) and externally (TSA.gov, DHS.gov, etc.) to answer:
  - What information is currently being captured
  - Where is the information being captured, stored, and used
  - How is the information being utilized and captured
  - Does the data interface, or is it shared, with other systems/services or offices
- The research expanded upon the initial list and identified other systems/programs that leveraged biometric data and respective Points of Contacts (POCs) for each
- A series of data calls to the POCs (direct emails, data calls, phone interviews, etc.) was conducted to complement, update, and prove the information found in the documentation research

Current State Architecture

Categorizing Biometric Functions

- In the context of this study:
  - **Biometrics** refers to a measureable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition of an individual
  - **Biographic** refers to the metadata (raw data) derived from biometrics to identify a person
  - **Capture** refers to the process taken by a system or program to physically take biometric information from an individual (e.g. obtaining fingerprints or facial images)
  - **Collect** refers to the actions taken by a system or program to leverage biographic data already captured by another system (e.g. a system that transmits biometric data from another system for vetting purposes)
- Four main functions will be used to define each system/program

Biometric Function	Description
Enrollment	Biometric information from an individual is captured
Verification	One-to-one authentication of a person's biometric trait (e.g. fingerprint, iris, face, etc.) to an enrollment record (e.g. smartcard, database, etc.) or database (e.g. IAFIS, IDENT, etc.)
Identification	One-to-many authentication of a person's biometric trait to an enrollment record or database
Storage	Biometric information from an individual is stored

Current State Architecture

TSA Systems & Programs that Leverage Biometric Information

The current TSA biometric landscape presents:

- **6** systems that handle **enrollment**
- **11** systems that handle **identification**
- **6** systems that handle **verification**
- **3** systems that handle **storage**

Current State Architecture

Ongoing & Future Projects/Pilots

- Projects disclosed here are still in the prototype/planning stages and have not yet been completely implemented and approved at TSA

Project	Description	Goal	Status
CBP-TSA Biometric Exit Program	Mandated by Presidential Executive Order and various federal statutes, Biometric Exit will allow CBP to track travelers leaving the country accurately through facial recognition	Increase security and improve screening process and passenger experience	Ongoing
Biometric Authentication Technology (BAT)	BAT verifies identity by matching fingerprints to a passenger's TSA PreCheck enrollment data and Secure Flight vetting status	Enhance security by changing the TDC from an administrative task to focus screening on higher risk efforts	Ongoing
Federal Air Marshal Service (FAMS) PIV Biometric Pilot	FAMS PIV Biometric pilot uses two factor authentication to validate identity at the checkpoint	Secure entry and identity validation of FAMS, LEOs and any armed passengers	Ongoing
Biometrics Integrated Project Team (IPT)	Originally formed in 2015, comprised of stakeholders representing offices across TSA and is currently being considered for refresh; the biometrics IPT is expected to enable other biometric Initiatives	Develop goals and a capability framework for biometrics	Ongoing
Known Crew Member Program (KCMP)	Verifies crew member access to various sensitive areas using biometrics	Combat insider threat and ensure secure access is granted to the proper crew members	Future
OSPIE - Delta Biometric Bag Drop	The Delta Airlines Biometric ID Verification at Bag Drop unit will access passenger passport photos for comparison to real time photos taken at the machine	Contribute to passenger experience and eliminate manual ID verification process	Future

Future State Recommendations & Strategy

Preliminary Strategic Goals/Roadmap

Interagency Collaboration

- Reduce friction with passengers through collaboration efforts, working to provide a seamless experience through checkpoint
- Identify opportunities for agencies to share identification/verification services, processes, strategies, and overall population data

Enhance Effectiveness of Subject Identification

- Consolidate/improve biometric collection systems
- Receive/centralize access to federal and international biometric databases with support and input from other agencies
- Implement systems with multi-modal use for scalability (facial, palm, iris, fingerprint, etc.)
- Expand use of biometrics outside of checkpoint (employee access, screening, bag drop, etc.)
- Automate resource intensive identity processes to reduce human dependencies
- Implement person-centric biometric processing
- Expedite security processes using identity verification capabilities

Refine Processes & Policies to Promote Innovation

- Joint requirements efforts – follow DHS guidance and reduce redundant work
- Establish TSA-wide biometrics authorities (governance, policy, legal authority, etc.)
- Develop privacy policies and processes – use DHS policies to inform TSA privacy policies for maintaining PII and leveraging biometric/biographic data
- Enhance stakeholder communications across TSA, DHS, and relevant agencies
- Implement standardized solutions across components (DHS, CBP, airlines, etc.)

Biometric Study Gaps & Next Steps

Disclosing confidence levels of information and future actions

Current Gaps:

- EAIR and iShare were considered the closest “sources of truth” for the information in this study
- Some of the information found in this study might be outdated—some discrepancies were identified during the research (e.g. Communications with Ratan Shah disclosed LEDA/e-Agent was decommissioned but SELC status on EAIR is “operational”)
- Information interfacing and being transmitted to/from systems was considered for general data—there is no clear distinction of the type of data that is shared to identify if its biometric/biographic or not as of right now
- Missing system information has been highlighted in yellow for future research

Next Steps:

- Research missing system information and update any outdated data
- Communicate final findings with system owners and biometric SMEs to corroborate information before distribution
- Creation of other views if needed
- Drill down on system/program information to understand if interfacing data is actually biometric/biographic