



Phillip Loranger
Ch Access Enabling Technology Team
Information Systems Security
Federal Aviation Administration
800 Independence Ave, SW
Washington, DC 20591

202-493-5063
Phillip.Loranger@FAA.Gov
14 Feb 02

1



Purpose

- **Discuss agency-wide strategy to achieve the FAA mission for access enabling technologies.**
- **Introduce GO team 36 access enabling technologies.**

2



Why an FAA Access Enabling Technology Team? (FAETT)

- Established on 2 Dec 2001 -
- Maximize Return On Investment (ROI) and achieve cost savings/avoidance by leveraging, coordinating and orchestrating efforts.
- Achieve enterprise-wide security standards in the following areas:
 - Positive verification and control
 - Authentication
 - Non-repudiation
 - Confidentiality
- Recent and pending congressional security mandates.

3



What's A Access Enabling Technology Team

- A very specialized teams to address technologies for business processes for integrations department wide.
- A Team that can and does support broad agency and department Access Security solutions for both Physical and Logical Access requirements.
- The FAA CIO leads this FAETT –
 - Smart Card development
 - PKI development
 - and Biometrics development

4



FAA Access Enabling Technology Team (FAETT)

→ **Vision:**

Establish Universal Positive Verification and Control for all Personnel and Entities Across the Agency's Full Spectrum of Transportation Operations to Ensure the Safety of the Flying Public

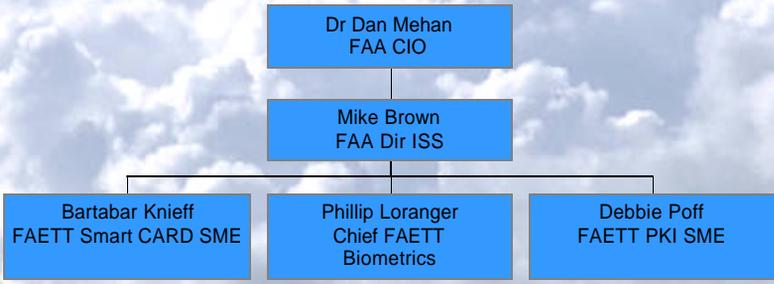
→ **Mission:**

Incorporate Access Enabling Technologies to help achieve enterprise security throughout the Agency's full spectrum of Transportation Operations where all personnel will have a single device using an infrastructure which is interoperable, extensible and scalable.

5



DOT / FAA Access Enabling Technology Team (FAETT)



```
graph TD; Mehan[Dr Dan Mehan  
FAA CIO] --- Brown[Mike Brown  
FAA Dir ISS]; Brown --- Knieff[Bartabar Knieff  
FAETT Smart CARD SME]; Brown --- Loranger[Phillip Loranger  
Chief FAETT  
Biometrics]; Brown --- Poff[Debbie Poff  
FAETT PKI SME];
```

6



Why a FAETT?

- ➔ **Maximize Return On Investment (RIO) and achieve cost savings/avoidance by leveraging, coordinating and orchestrating efforts.**
- ➔ **Achieve department enterprise-wide security standards in the following areas: (Token Based)**
 - **Positive verification and control**
 - **Authentication**
 - **Non-repudiation**
 - **Confidentiality**
- ➔ **Recent and pending congressional security mandates.**

7



FAETT Questions Verified access can it be done

???????????

- **Who are you & can you prove it,**
- **Is your biometrics really you,**
- **So who are you,**
- **Now prove it,**
- **Make me believe it,**
- **How do I adjust to who you are and**
- **Is there a better way**

8



WHAT IS OF INTEREST TO US

- Any Non Cooperative positive verification and authentication technologies
- 3 to 7 second registration process
- 2 or more token production at the same time (I.E. boarding pass and baggage tag)
- 3- 7 min database interactive checks between boarding environments and national databases (Rough amount time a passenger, who is in a hurry, to get from counter to boarding gate.)
- TOTAL interoperable creditably verification across the entire transportation industry.

9



What Is FAA Looking at in a Smart Card?

A Credit Card-Sized Device That May Hold:

- Integrated Circuit Chip (ICC) 32/64
- Magnetic Stripe
- Bar Codes
- Photo Identification
- Encryption and Authentication
- Biometrics
- 2 Dimensional Barcode
- Non-Contact Radio Frequency Transmitter









10



How May the FAA Smart Cards Work?



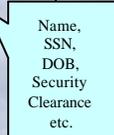
Smart Cards start as blank plastic cards that contain an Integrated Circuit Chip (ICC). Business or operational requirements determine which additional technologies that will be contained on the smart card and drive the surface topology.

To make the blank card into an ID Card, an individual's photograph and specific personal demographic data about that individual is added to face of the smart card and can be stored securely on the ICC.

Once the ICC on the card has been initialized with the individual's personal demographic data, the card can be used for operations or with applications that require positive personnel verification and control (facilities access system or logical access system) via a smart card reader to verify the individual's identity.



Michael Brown
Dir. Information Systems Security






11



WHAT BIOMETRICS MEANT FAA BE INTERESTED FOR INTEGRATION?



Biometrics are measurable physical characteristics or personal behavioral traits used to recognize the identity, or verify the claimed identity of an individual.





facial recognition, fingerprints, hand/finger geometry, iris scan, signature verifications, speaker recognition and portal biometri






12



What Public Key Infrastructure (PKI) Meant FAA Be Looking For?

Public Key Infrastructure. A Public Key Infrastructure (PKI) which includes people, policy, procedures, hardware and software components, and facilities necessary to enable public key encryption and digital signatures, so that applications can provide the desired electronic commerce and security enhancements.



Public Key Encryption. A cryptographic process using two mathematically related keys (one held privately, the other available publicly) for encrypting and decrypting electronic transactions, and creating and validating digital signatures



Digital Signature. A secure hash process using public key cryptography whereby a user can electronically sign an electronic transaction. The digital signature can be validated as genuine and the signed transaction cannot be altered without detection.



13

11000101001100100100111010



DOT GO Team 36

- **Team Chair Mr. Mike Brown AIS-1**
- **Issue: Smart Card Technology
Position for TSA**
- **Charge: Develop the framework for identifying and evaluating various smart card technology solution options for FAA and DOT personnel**

14



FAA's FAETT Near Term Goals

- **Ensure Interoperability of Smart Card buys for FY02.**
- **Define layout of the baseline Enterprise-wide Smart Card by Mar 02.**
- **Define technologies for inclusion on the Enterprise-wide Smart Card by Mar 02**
 - **Magnetic strip, bar code, image, etc.**
 - **Integrated Circuit Chip (ICC) capacity/content**
 - **Top level chip allocations for password, PIN, Biometric, and PKI certificates**
- **Ensure scalability of smart card for follow on I&A, verification, encryption, and control and use by FAA / DOT MOD's and Staff.**

17



FAA's FAETT Near Term Goals

- **Baseline for Card requirements based on assumptions.**
- **Draft Arch and Standards (SC/PKI/BM/Laser Strip)**
 - **Draft timeline for tasks to meet GO Team deliverables.**
 - **Draft breakout of the DOT/TSA Data Model**
 - **Provide a listing of issues and recommendations for success.**

18



FAA's FAETT Long Term Goals

- **Define an integrated Architecture that incorporates Smart Card, PKI and Biometrics.**
- **Continue providing advice and assistance to FAA Program Managers for the implementation of access technologies for both legacy and new starts.**
- **Continue Departmental effort with DOT CIO's Office and DOT's TSA GO Teams.**

19



Business Process GO TEAM Responsibilities

- **Centralized Implementation Management and Oversight: GO Team 51**
 - Card Management and Issuance
 - Infrastructure Fielding
- **Enabling DOT Applications to use Smart Card Technology: All DOT Functional Proponents**
 - Application Applet Development
 - Submission of ECPs to DOT CMB
 - Fielding of required application readers
- **Centralized Management and Oversight: GO Team 36 / 51**
 - Card Architecture, Standards and Policies
 - Configuration Management of the Technology

20



How can the Access Enabling Industry help

- **Agree that no single access technology meets requirements**
- **Seek Outreach with DOT / FAA**
- **Join and support national and international standards groups**
- **Partnerships with FAA Technical Centers**
- **Discuss possible pilots with us**
- **Get EAL (3) & FIPS 140-1 level 2 ratings for your products**

21



Summary

- **Leverage our desire, our staffs and the industry to acquire, integrate, and deploy access technologies that maximize our ROI.**
- **Multiple current initiatives within the FAA that are developing independent security solution sets, within several LOBs.**
- **The FAETT has the required SMEs to develop the needed plans to organize and orchestrate an enterprise-wide solution set for the FAA.**
- **National mandate to enhance our business process security across centers of operations agency and department wide.**

22



Contacts

| <u>Name</u> | <u>Phone</u> | <u>Email</u> |
|------------------|--------------|--|
| Phillip Loranger | 202 493-5063 | phillip.loranger@faa.gov |
| Barbara Knieff | 202 267-5673 | barbara.knieff@faa.gov |
| Debbie Poff | 202 493-5432 | deborah.poff@faa.gov |

23