



The TSA Registered Traveler Program

Biometrics Consortium Conference, 2006

Conor White, CTO, Daon

RT Interoperability Consortium (RTIC) An Overview



- **Created in June 2005**
- **Members**
 - 68 airports and airport authorities
 - 47 service providers
- **Objective**
 - Develop the common set of technical standards and processes necessary for an open, secure and industry-driven RT program



What is Registered Traveler?



- A privilege program that expedites the passage of travelers through participating airports
- Uses smart cards and biometrics to assure a person's identity at the airport
- Participation requires enrollment with a Service Provider
- TSA will perform a Security Threat Assessment
- A Central Information Management System (CIMS) will
 - Ensure interoperability across Service Providers
 - Generates the biometric templates for the RT card
 - Digitally signs the authentication data on the RT card
 - Maintains and propagates the CRL
- RT is a public/private partnership
- Fully fee funded



© Copyright 2006, Daon.

3

Key Business Requirements



- Registered Traveler has a number of Key Business Requirements
 - Protect Privacy
 - Ensure a Chain-of-Trust throughout
 - Avoid PINs
 - Align with PIV to the greatest practical extent
 - Support finger and optionally iris
 - Provide interoperability across all vendors and airports
 - Minimize Costs



© Copyright 2006, Daon.

4

Developing the Specification



- Dedicated “War room” team
- Met three days per week in Reston, VA
- Specification started early May
- Participants included:
 - Service Providers
 - Technology Providers
 - Consultants
 - TSA liaisons
- A number of formal reviews took place bringing inputs from other key stakeholders – e.g. DHS, NIST.
- Final Specification submitted **YESTERDAY!**
- An amazingly fast development time
- Full credit goes to the members of the RTIC war room team



The War Room team

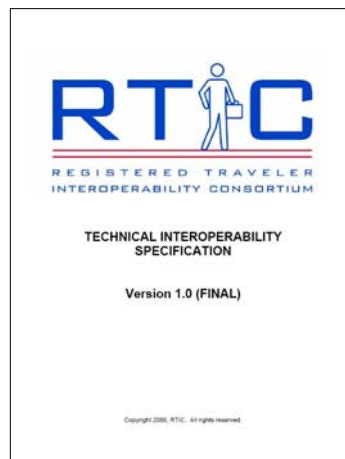


- | | |
|---|---|
| • Gena Alexa, Unisys | • Daniel Daehoon Kim, Iritech |
| • Dave Auman, ID Technology Partners, TSA Liaison | • Gilles Lisimaque, ID Technology Partners, TSA Liaison |
| • Jamon Bailey, Saflink | • Bill McCann, ImageWare |
| • Jim Cambier, Iridian Technologies, Co-Editor – Biometric Management and Use | • Travis McCoy, Saflink |
| • Patricia Carbone, MITRE Corporation, TSA Liaison | • Tim Meyerhoff, LG Iris |
| • Colleen Chamberlain, AAAE, Co-Editor – Concept of Operations | • Rajan Ramasamy, AAAE |
| • Larry Cleary, Iridian Technologies | • Ryan Regensburger, Lockheed Martin, Editor - System Security |
| • Ali Ezzati, Lockheed Martin | • Jerry Ruddle, Iridian |
| • Jason Goodloe, Daon, Co-Editor - System Messaging | • Eileen Sexton, ImageWare |
| • Vadim Grinshpun, Unisys, Co-Editor - Conformance | • Jason Slibeck, Verified Identity Pass, Co-Editor - Conformance |
| • Richard Hite, Teragon Consulting | • Matthew Swayze, Daon, Co-Editor - Biometric Data Management and Use |
| • Chris Holland, Saflink, Co-Editor - Concept of Operations | • Cathy Tilton, Daon |
| • Bryan Ichikawa, Unisys, Editor - RT Card | • Steve Venable, Lockheed Martin, Co-Editor - System Messaging |
| • Travis Jaeger, Iritech | • Andrew Webb, Daon |
| • David Johnston, LG Iris | • Conor White, Daon, Chair - RTIC Technical Interoperability Working Group, Editor-in-Chief |

- **The RT Card leverages to the greatest practical extent the FIPS 201 standard**
 - We use the same card edge interface
 - We use the same security objects on the card
 - Much of the biometric data management requirements (SP 800-76) have been adopted.

- **However**
 - RT does not use PINs
 - RT supports 4 fingers on the card
 - RT supports the optional use of iris
 - RT does not use a contactless interface
 - RT is not a federal credential

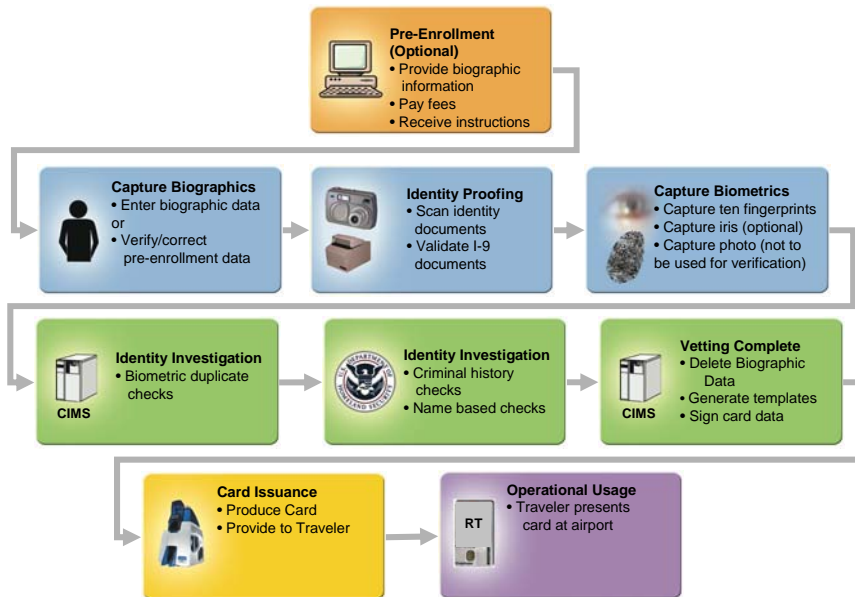
- **Covers 7 sections:**
 1. Introduction & Overview
 2. Concept of Operations
 3. Biometric Data Management & Use
 4. System Messaging
 5. RT Card Model
 6. System Security
 7. Conformance Testing Principles



- **The specification is available for download from:**

<http://www.rtconsortium.org/>

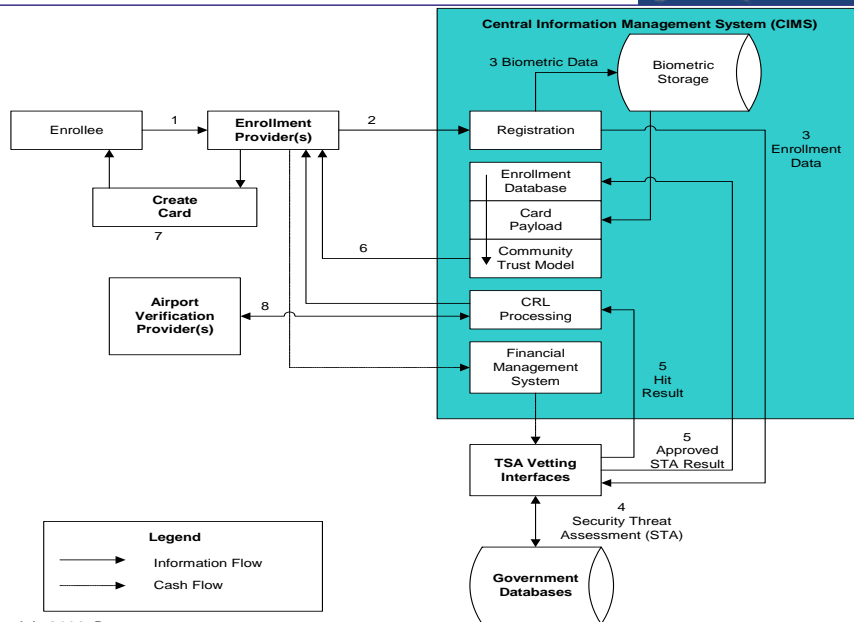
The RT Process – In a Nutshell



© Copyright 2006, Daon.

9

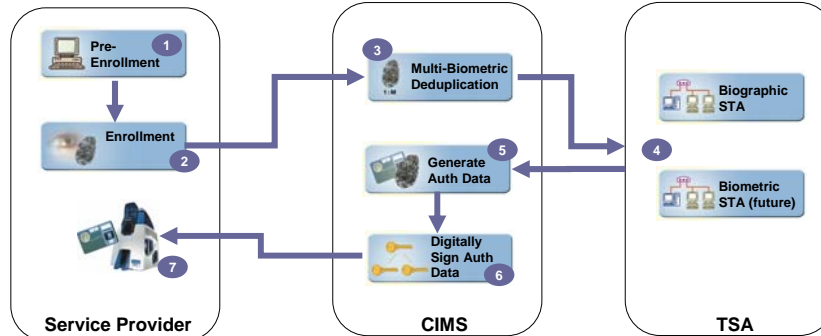
Core Components and Information flows within the RT Program



© Copyright 2006, Daon.

10

Enrollment Processing Overview (Simplified View)



1. Customer provides biographic data at (optional) pre-enrollment phase
2. Service Provider collects biometric data and forwards enrollment record to CIMS
3. CIMS receives enrollment data, performs quality checks, multi-biometric deduplication
4. CIMS provides data to TSA vetting gateway. TSA performs Security Threat Assessment (STA)
5. On successful STA, CIMS generates card authentication data from enrollment data
6. CIMS digitally signs the authentication data to prevent tampering and returns to Service Provider
7. Service Provider produces card and provides to Traveler

© Copyright 2006, Daon.

11

Biometrics within RT



■ Fingerprints

- Ten slap prints at enrollment
- Four fingerprints on RT card - INCITS 378-2004

■ Iris

- Optional capture of two iris
- Rectilinear format for enrollment and storage at CIMS
- Unsegmented polar image format for RT card
- Compliant with ISO/IEC 19794-6:2005

■ Face

- Captured at enrollment
- ANSI INCITS 385-2004
- Stored on card, NOT used for authentication!

© Copyright 2006, Daon.

12

Security and Privacy of Data objects



Data Object	Read access	Signed by
RTUID – Payload Id	Free	CIMS and Enrollment Provider
Finger1 Biometrics	Mutual Auth with HSM	CIMS
Finger2 Biometrics	Mutual Auth with HSM	CIMS
Iris Biometrics	Mutual Auth with HSM	CIMS
Facial Image	Mutual Auth with HSM	CIMS
Other Data	Mutual Auth with HSM	
RT Preferences	Free	
ICAO Security Object	Free	CIMS

© Copyright 2006, Daon.

13

Why is RT Card data secure and private ?



- The RT card data is signed by CIMS to prevent counterfeit biometric data being used and also to bind all the data objects together.
- A HSM in the VP station mutually authenticates with the RT card to allow only VP stations to read the biometrics and to also validate the RT card to the VP station.
- The HSM itself must be activated securely.
- RT card application is *contact only, and no authentication information is modified* after issuance.

© Copyright 2006, Daon.

14

Thank You

Questions?

**Email: conor.white@daon.com
Tel: 703 984 4010**