TECHNICAL INTEROPERABILITY SPECIFICATION

Version 1.5

December 21, 2007

Document Disclaimer

The information contained in this specification represents the current consensus views of the Registered Traveler Interoperability Consortium (RTIC) members on the issues discussed herein as of the publication date. Because TSA may change any of the preliminary RT specification requirements, no part of this document should be interpreted as a commitment on the part of the TSA, or the RTIC, to any part of the RT Program described in this document.

The contents of this document are for informational purposes only and do not constitute or represent a legal document or agreement. The RTIC makes no guarantees as to the accuracy or completeness of the information in this document.

The examples depicted herein are for illustrative purposes only and are in no way intended to be associated with any real company, organization, product, or person.

Copyright Notice

The information in this document is subject to change without notice. We welcome user comments and reserve the right to revise this publication at any time.

The information in this document is provided as is, where is, with any and all faults included, and without any representations or warranties of any kind (express, implied, oral or written), including, but not limited to, representations and warranties of non-infringement, merchantability and fitness or suitability for any particular purpose, whether alleged to arise by law, custom or usage in the trade, or course of dealing.

This document may contain technical inaccuracies or typographical errors. The copyright holders are not liable for any direct, indirect, special, or consequential damages arising out of any use of this document or the performance or implementation of the contents thereof.

Should any viewer of this document respond with information including feedback data, such as questions, comments, suggestions, or the like regarding the content of any such document, such information shall be deemed to be non-confidential and the RTIC shall have no obligation of any kind with respect to such information and shall be free to reproduce, use, disclose and distribute the information to others without limitation. Further, the RTIC shall be free to use any ideas, concepts, know-how or techniques contained in such information for any purpose whatsoever including but not limited to developing, manufacturing and marketing products incorporating such information.

Revision History

Version	Date	Description
1.0	21 Sep 2006	Original/baseline specification submitted to TSA
1.1	5 Mar 2007	Updates based on conformance testing
1.1	30 Mar 2007	Updates based on comments received from TSA and RTIC meetings
1.2	May 2, 2007	Changes to clarify iris quality processing at EP and CIMS

1.3	16 Oct 2007	Additions and clarifications related to capture equipment information, CRL expiration, subpopulation handling, minimum good fingers, and POB/citizenship fields.
1.4	12 Nov 2007	Facial photo and name made mandatory for printing on front of card. Key rollover requirements modified.
1.5	21 Dec 2007	Removed changes associated with inclusion of photo on front of card pending TSA decision. Incorporated TSA comments related to best effort prior to granting of waiver, mandatory inclusion of citizenship status, auditor recommendations on KM rollover, and conformance requirements.

Table of Contents

1 Introduction and Overview

This section provides an introduction and overview of the RTIC Technical Interoperability Specification.

1.1 Background

This document is the technical interoperability specification for the US Registered Traveler program. This document was developed by the Registered Traveler Interoperability Consortium (RTIC) to help foster a fully-interoperable, vendor-neutral Registered Traveler (RT) program within the United States.

This document is divided into seven sections as follows:

1. Introduction and Overview	Covers introductory material including the RTIC, the specification development process, major business requirements that drove key technical decisions and a summary of the differences between RT and the Personal Identity Verification (PIV) program.
2. Concept of Operations	Provides an overview of the major processes within the RT system including a diagrammatical and procedural description. Introduces many of the key concepts within the RT program.
3. Biometric Data Management and Use	Details the biometric standards for enrollment, verification, storage and transmission of biometric data.
4. System Messaging	Details all major messages between components in the RT program including the Enrollment Providers, Verification Providers and the Central Information Management System (CIMS).
5. The RT Card	Outlines the smart card application structures, interfaces and security protocols.
6. System Security	Details the security guidelines and principles for the RT program and covers the logical and physical security of areas not covered elsewhere in this specification.
7. Conformance	Outlines some high level guidance on how conformance testing will be done within the RT program. Note: This does not cover detailed conformance tests at this point.

Before reading any of Sections 3 through 7, it is highly recommended that readers first familiarize themselves with Sections 1 and 2.

Please note: All comments are welcome. Please email any comments to conor.white@daon.com.

1.1.1 Introduction to the RTIC

The Registered Traveler Interoperability Consortium (RTIC) was formed by a group of airports in conjunction with the American Association of Airport Executives (AAAE) in June 2005. Recognizing the value of the registered traveler concept, the airports agreed to work together to leverage existing airport resources and the AAAE's Transportation Security Clearinghouse (TSC) to facilitate a permanent, interoperable and vendor-neutral RT program in the United States.

A permanent, interoperable RT program depends on the implementation of a technical, operational, and business model capable of supporting the needs of individual airports, while providing the common infrastructure that allows passengers to use this capability at any participating airport. As a result, the main objective of the RTIC is to develop the common set of technical standards and processes necessary for an open, secure and industry-driven RT program.

In October 2005, the airport members of the RTIC announced the formation of a Service Provider Council. The Service Provider Council was established as a way for service providers to participate in the development of the technical standards and processes required for an interoperable RT program. To focus the attention and participation of the Service Provider Council members, three working groups were formed:

1. **Technical Interoperability Standards Working Group** – This group (known as TIG) worked to establish a technical interoperability standard that enables the inclusion of any airport and any service provider into a national RT program.
2. **Common Business Processes Working Group** – This group worked to define and document the operational steps for RT service providers for enrollment, vetting, RT card issuance, checkpoint verification and reporting and a standard process for security checkpoint operations for designated and dedicated RT lanes.
3. **Financial Standards Working Group** – This group worked to provide recommendations for the setting of a basic service fee structure and the associated operational processes for fee transfer between RT service providers.

The Service Provider Council draws on the expertise and experience of over 40 well-known and respected commercial organizations that specialize in, among other things, Registered Traveler solutions, smart cards, biometrics, identity management, security, and airport management.

In January 2006, the RTIC and its Service Provider Council submitted three detailed responses to the TSA's request for information on RT (TSA Solicitation #21-06-206TTC000) on 1) technical interoperability, 2) common business processes and 3) financial standards. The RTIC responses outlined a consensus framework for the rapid deployment of a sustainable, biometrically enabled and interoperable RT program. In addition, the RTIC responses detailed a public-private business model that utilizes a non-proprietary, open-architecture approach and creates a fair and seamless platform for airports, airlines and RT service providers to interface with the TSA and among each other.

1.1.2 Development of this Specification

In April 2006, to follow-up on the consensus response to the TSA RFI, the RTIC and its Service Provider Council began to focus its efforts on defining the technical specification needed for an interoperable RT program. The Technical Interoperability Working Group of the RTIC Service Provider Council established a war-room environment in Reston, Virginia, working face-to-face three days a week, to define and draft

the technical specification for the RT program. TSA encouraged interested stakeholders to join in this effort.

The war-room team, which consisted of approximately 25 individuals, divided the task of drafting the technical interoperability specification into sections and selected by consensus editors and co-editors for each section. The war room team, as a whole and in sub-groups, worked on content creation, and the editors and co-editors were responsible for the management of their section.

The team used the RTIC submissions to TSA Solicitation #21-06-206TTC000 and the TSA's Registered Traveler Model (released on May 25, 2006) as a basis for assumptions regarding the structure of the RT program. The team also aimed to leverage existing National and International standards to the greatest practical extent. Major issues and decision points not already outlined in either the TSA RT Model or the RTIC submissions were discussed in an open forum of all in-person members. When unanimous verbal agreement could not be reached, a question was sent to TSA for resolution. All questions to the TSA and responses were documented and are available for review. The TSA's Registered Traveler Program Office provided liaison staff who attended the meetings and worked closely with the war-room team to provide guidance and direction regarding major issues and assumptions.

Drafts of the technical interoperability specification were distributed to the full Technical Interoperability Working Group (in addition to those present in the war-room) for review and comment. After each review period, the war-room team formed a disposition on each comment. Again, comments on the draft specification and the disposition of the comments were documented and are available for review.

This document is a result of the RTIC Service Provider Council's Technical Interoperability Working Group's efforts. It is presented to TSA on behalf of the entire RTIC and provides a consensus framework for the rapid and secure deployment of a permanent, interoperable and vendor-neutral RT program in the United States.

1.1.3 Specification Development Team

Many people within the RTIC were involved in the creation and review of this document. Throughout the process, the broader RTIC Technical Interoperability Group was involved in ongoing reviews and input.

In particular, the following people were the core team directly involved in the war-room activity:

- Gena Alexa, Unisys
- Dave Auman, ID Technology Partners, TSA Liaison
- Jamon Bailey, Saflink
- Jim Cambier, Iridian Technologies, Co-Editor – Biometric Management and Use
- Patricia Carbone, MITRE Corporation, TSA Liaison
- Colleen Chamberlain, AAAE, Co-Editor – Concept of Operations
- Larry Cleary, Iridian Technologies
- Ali Ezzati, Lockheed Martin
- Jason Goodloe, Daon, Co-Editor - System Messaging
- Vadim Grinshpun, Unisys, Co-Editor - Conformance
- Richard Hite, Teragon Consulting

- Chris Holland, Saflink, Co-Editor - Concept of Operations
- Bryan Ichikawa, Unisys, Editor - RT Card
- Travis Jaeger, Iritech
- David Johnston, LG Iris
- Daniel Daehoon Kim, Iritech
- Gilles Lisimaque, ID Technology Partners, TSA Liaison
- Bill McCann, ImageWare
- Travis McCoy, Saflink
- Tim Meyerhoff, LG Iris
- Rajan Ramasamy, AAAE
- Ryan Regensburger, Lockheed Martin, Editor - System Security
- Jerry Ruddle, Iridian
- Eileen Sexton, ImageWare
- Jason Slibeck, Verified Identity Pass, Co-Editor - Conformance
- Matthew Swayze, Daon, Co-Editor - Biometric Data Management and Use
- Cathy Tilton, Daon
- Steve Venable, Lockheed Martin, Co-Editor - System Messaging
- Andrew Webb, Daon
- Conor White, Daon, Chair - RTIC Technical Interoperability Working Group, Editor-in-Chief

1.2 Key Business Drivers for the RT Program

The TIG is tasked with developing the technical interoperability specification that conforms to the key business requirements of the RTIC. These overarching business requirements are defined by the Common Business Processes Group within the RTIC. Some of the key requirements put forth by this group that affected our technical choices and the resulting specification are outlined below. The purpose of outlining these is to give the reader an understanding of the key business principles that drove some of the technical choices that were made in this specification.

While the RTIC TIG attempted to adhere to industry standards wherever possible, variances from those standards were required in some cases due to requirements that are unique to the RT program.

1. **Protect Privacy**

   With the increase of identity theft in today's world, one of the primary concerns of the RTIC is protecting consumer privacy. The RTIC specification establishes privacy controls that will set industry best practices for protecting consumer privacy rather than just a minimum baseline. Privacy controls include:

   a. Preventing an unauthorized entity from reading RT applet biometrics.

   b. Preventing a Service Provider (SP) from tracking RT activity at security checkpoints.

c. Providing assurance and protection of all data in transit and at rest.

d. Storing only the minimum data required on the card to complete an RT transaction.

e. Using comprehensible and concise language to request informed consent from RT Applicants to opt-in before an Enrollment Provider can store, use, share and/or sell biographic or biometric data obtained for the RT program.

f. Preventing unauthorized storage, use, sharing, or selling of biographic or biometric data by Enrollment Providers acquired for the purpose of the RT program.

Furthermore, members are concerned not only with real privacy threats, but also perceived issues (whether technically valid or not). For example, in the earliest stages of this work, the business group determined that they did not want to support a contactless card for this release due to the perception among many that contactless tokens constitute a privacy risk. Technically, these risks can be minimized; however, changing the perception will require a significant market education effort which the RTIC members cannot undertake at this time.

The RTIC technical team is aware that with the appropriate authentication protocols, contactless smart card technology is a legitimate and secure technology that should be considered for use in the RT program in the future.

Two important privacy concepts are the VID and the access control rules for the RT card application.

a. Verification ID (VID)

The VID concept was created to meet the privacy requirement that an RT Participant's activity is not tracked at the verification station. The VID allows each Verification Provider (VP) to record unique transactions at the verification station through the VID while still maintaining anonymity of the RT Participant. Each Enrollment Provider will be required to provide a transfer fee to the Verification Provider when an RT Participant from that Enrollment Provider uses the verification station. In order for the Verification Provider to provide a list of transactions, they must record a minimum amount of data for the verification event. The use of the VID allows the Verification Provider to record a unique transaction record without tying that transaction to a specific RTID. More information is provided in Section 2, Concept of Operations.

b. Access Control Rules

Preventing an unauthorized entity from reading RT applet biometrics is one of the primary privacy controls identified by the RTIC TIG. Since PINs were identified as impractical for card user authentication, another means of protecting biometric data on the RT applet is required. As a result, the RTIC TIG determined that for a distributed RT program with multiple providers, the best approach to protecting biometric data on an RT applet should be through a mutual authentication scheme using diversified keys. More details are provided in Section 5, The RT Card Model, and Section 6, System Security.

2. Avoid PINs

One of the primary goals of the RT program is to speed the passage of travelers through the airport security checkpoints. Unlike logical or physical access control solutions which may require employees to use their credential on a daily basis, RT Participants may use cards as infrequently

as once per month. As a result, using PINs to authenticate a user to the RT card is not practical. Using a PIN to access the card will result in users forgetting their PIN which will in turn negatively impact throughput through the RT checkpoint. An even worse scenario would arise if users begin to write their PIN on their card. As a result, the use of PIN-based authentication to the RT card was deemed unacceptable for the RT program, and an alternative card authentication method was chosen.

3. **Minimize Costs**

   Unlike many of the government-funded credentialing and security programs, the funding for the RT program is provided solely by private entities. For each airport, Enrollment Providers are required to provide the infrastructure, equipment, software and staff to support the enrollment process. Verification Providers are required to provide all of the infrastructure, equipment, software and staff to support the verification process. These Service Providers recover costs through enrollment fees provided by the RT Applicants and usage of verification stations. As such, a primary concern for all Service Providers is that the lowest cost solution be defined that will meet the security, privacy and functional requirements of the RT program while limiting upfront investment.

   For example, the RTIC Common Business Processes Working Group requested that the use of PKI be minimized due to the cost and complexity issues associated with it for large scale programs – the potential enrollment population for RT could reach over 20 million people.

1.3 The Relationship between RT and PIV

There are some similarities between the RT program and the Personal Identity Verification (PIV) program. Utilizing biometric and smart card technology, the PIV program implements a secure and reliable form of identification for Federal employees and contractors. To the greatest extent practical, this specification has attempted to leverage the PIV specifications. However, there are also some significant business requirement differences that make the RT card different from a PIV card. This section outlines some of the key deviations from PIV and the reasons for them.

1. **RT Participants do not use PINs.**

   Participants in the RT program will not use PINs to authenticate themselves. Even the most frequent travelers will not always remember their card PINs. Furthermore, requiring users to enter a PIN or passphrase will slow down the authentication process at the verification station and increase the length of lines, resulting in unacceptable increases in the level of exception handling required. All Service Providers within the RT program want to use biometrics alone (without a PIN/passphrase) to authenticate the travelers. As a result, the RT card will not use PIN-based authentication to card contents.

2. **RT Participants will optionally use iris to authenticate themselves.**

   The RT business model from the TSA states that iris may be optionally used for authentication. This decision was taken based on evidence from the initial airport pilot programs which indicated that iris was a biometric that many travelers preferred. PIV does not support iris as a reference biometric, and the RT program allows it as a verification option.

3. **The RT program allows up to four fingerprint templates to exist on the RT card.**

   Based on experience in the pilot deployments, it is believed that providing four fingerprint templates on the card is necessary to minimize issues with using verification stations (i.e., reducing system-level false rejections). The PIV program only allows two fingerprint templates on a card, whereas RT requires four.

4. **The RT program does not use contactless tokens.**

   For any RT transaction, the biometric data must be read from the card to authenticate the RT Participant at the security checkpoint. As such, leveraging the PIV contactless interface did not provide a benefit to the RT program since the biometric data is not accessible through the contactless interface in PIV. While the RTIC TIG discussed exposing the biometrics through the contactless interface, it was determined that for the initial rollout of the RT program, contact only cards would be used due to perceived privacy issues and a significant cost difference between contact only cards and dual interface cards.

5. **The RT card is not a federal credential.**

   The RT card is not a federal credential and is not allowed to be used as such. There is no requirement to integrate with the Federal PKI Bridge. As a result, the PKI and FIPS 140-2 requirements of the RT card are different from that of PIV.

Although there are differences between the RT and PIV programs, it is important to recognize that the RT technical specification leverages, to the greatest practical extent, the specifications developed for PIV. For example, the RT and PIV programs are aligned in the following ways:

1. RT uses the same fingerprint capture and quality management methods.
2. RT uses the same PIV card edge interface.
3. The RT specification allows the RT application to co-reside with PIV applications if necessary.

1.4 Intended Audience

This is a technical document which is designed to provide guidance to:

1. Organizations with oversight responsibilities related to the RT program (e.g., the TSA).
2. Sponsoring organizations hoping to implement an RT solution (e.g., airports).
3. Service Providers participating in the interoperable RT program.
4. Other engineering or technical personnel interested in the detailed technical operations of the RT program.

1.5 Related Documents

The following are some related documents for the interested reader:

- ANSI/NIST-ITL 1-2000, " Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information"
- Biometrics Security Technical Implementation Guide Version 1, Release 3, 11 Oct 2005 Developed by DISA for DOD
- Electronic Fingerprint Transmission Specification, Version 7.1

- Federal Information Security Management Act (FISMA) (P.L.107-347)
- ICAO Biometrics Deployment of Machine Readable Travel Documents, Technical Report, Version 2.0
- INCITS 378-2004, "Finger Minutiae Format for Data Interchange"
- INCITS 385-2004, "Face Recognition Format for Data Interchange"
- INCITS 398-2005, "Common Biometric Exchange Formats Framework (CBEFF)"
- ISO/IEC 10918, "Digital Compression and Coding of Continuous-Tone Still Images"
- ISO/IEC 15444, "JPEG 2000 Image Coding System"
- ISO/IEC 19794-6:2005, "Information technology – Biometric data interchange formats – Part 6: Iris image data"
- NIST Special Publication 800-73, "Interfaces for Personal Identity Verification (PIV)"
- NIST Special Publication 800-76, "Biometric Data Specification for Personal Identity Verification"
- NISTIR 7151, "Fingerprint Image Quality"
- Privacy Act of 1974, 5 U.S.C. Section 522a
- Registered Traveler Model published by TSA.
- "RTIC Conformance Testing Test Plan/Procedures"
- "TSA Registered Traveler Security, Privacy, and Compliance Standards for Sponsoring Entities and Service Providers"

1.6 Glossary of Terms

This section defines some of the terms used throughout the remainder of this document.

Term	Definition
AAAE	The American Association of Airport Executives.
Authentication Data Sequence Number (ADSN)	An identifier that forms part of the authentication payload. This identifier increases in value each time a payload is requested from the CIMS and is used to uniquely identify individual payloads/cards (e.g., for card level revocation).
Authentication Payload	The block of data generated by the CIMS (and securely stored on the card by the enrollment SP) that is used to authenticate an individual within the RT program.
Card ID	A combination of the SPID, RTID and ADSN.
Central Information Management System (CIMS)	A system to aggregate, store, and distribute information (on an as needed basis) to the entities participating in RT.
Card Revocation List (CRL)	A digitally signed list of revoked or suspended entities. Each element of the list is composed of SPID or SPID+RTID or SPID+RTID+ADSN.

Term	Definition
Deletion of Data	Requires the data file to be completely overwritten without ability to reconstruct a record in whole or in part.
Duplicate Check	The process of identifying cases where a new enrollment may already exist under the same or different identity within the system.
Enrollment Provider (EP)	An RT Service Provider that collects the biographic and biometric information from RT Applicants, collects user fees from RT Applicants, and issues RT cards to RT Participants. An Enrollment Provider may be the same entity as a Verification Provider.
Globally Unique Personal Identifier (GUPID)	The identifier used by the TSA to uniquely identify an individual during multiple vetting processes. The same identifier is used for any given individual across all Service Providers.
Payload ID	This is a compound field composed of the SPID, RTID, ADSN and an expiration date. The expiration date is the date before which the TSA expects a resubmission of enrollment information for the traveler. This date is effectively the date on which the RT card expires.
Personal Identity Verification (PIV)	The PIV program implements a secure form of identification for Federal employees and contractors that meet the specifications developed pursuant to Homeland Security Presidential Directive (HSPD) 12.
Registered Traveler (RT)	Refers to the program or system as a whole; not to be used to refer to a participant in the program.
RT Applicant	An individual who has voluntarily supplied biographic and biometric data to an RT Enrollment Provider with the intent of joining RT and paying the associated user fee.
RT Card	The card issued to an RT Participant.
RT Conformance Lab	The entity responsible for ensuring that Service Providers comply technically and procedurally with the RT program's technical interoperability standards.
RTID	A 16 character identifier assigned by the Enrollment Provider and used to identity their RT customer. This identifier is always 16 characters long and is composed of uppercase characters A to Z, digits 0-9, "-" (hyphen) and "_" (underscore).
RT Line	A dedicated line before the security checkpoint where RT Participants queue for the verification process.

Term	Definition
RT Participant	An individual who has voluntarily enrolled with an Enrollment Provider, receives and maintains an approved STA from the TSA, and meets all other requirements set by the TSA.
RT TSA Security Lane	A TSA lane dedicated to RT Participants that have successfully passed the verification process at the verification station.
RTUID	An RT data object composed of the Payload ID and the VID.
Security Threat Assessment (STA)	A TSA process that includes checking the RT Applicant's information against terrorist-related databases, criminal databases for outstanding warrants, and other government databases that the TSA maintains or uses in order to confirm that volunteers are U.S. citizens, lawful permanent resident aliens or nationals of the United States, and to ensure that the volunteer does not pose or is not suspected of posing a threat to transportation security.
Service Provider (SP)	A term of collective reference for Verification Providers and Enrollment Providers.
Service Provider ID (SPID)	A unique identifier assigned to each Service Provider by the CIMS.
TSA	US Department of Homeland Security's Transportation Security Administration.
Transportation Security Clearinghouse (TSC)	An entity within the AAAE that acts as the CIMS for the RT program.
TSA Security, Privacy and Compliance Process	The process of approving an RT Service Provider's system such that they are in compliance with the TSA Security, Privacy and Compliance document (which is based on TSA standards for financial, security and process related functions). This is also known as the TSA Validation and Verification Process and referred to as the V&V process in this document.
TSA Vetting Interfaces	TSA-run information technology system(s) used to facilitate the STA and interface with the CIMS.
Verification Provider (VP)	An RT Service Provider that verifies the identity of the RT Participant in the airport in accordance with TSA-issued RT standards. A Verification Provider may be the same entity as an Enrollment Provider.
Verification Station	The device (typically a kiosk) used at the security checkpoint to verify the current status of the RT Participant and ensure that the card holder is the person to whom the card was issued.

Term	Definition
Verification ID (VID)	Verification Identifier – a value set by the Enrollment Provider on the RT applet that can be recorded by the verification station when the card is presented. Personal information must not be used to determine the value of the VID, or of any other IDs in the RT program.

2 Concept of Operations

The Concept of Operations section provides an overview of the fundamental aspects of the RT program. In addition to describing the key aspects of RT implementation, this section includes use cases that describe the processes by which the key components behave. Examples include the manner in which an applicant enrolls, how the applicant gets approved, and how the verification system functions.

2.1 Introduction to Key Concepts

2.1.1 Overview of RT Enrollment Process

An RT Applicant applies with a specific Enrollment Provider for participation in the RT program. Different EPs may provide different auxiliary benefits, but the core functionality of the RT program requires the submission of personal information (biographic and biometrics) for vetting. In order to fulfill this function, all EPs must satisfy core requirements with regard to enrollment.

Although there are exceptions and alternate functions (detailed in Section 2.4, RT Use Cases), the following figure serves to illustrate the processes involved in basic enrollment:

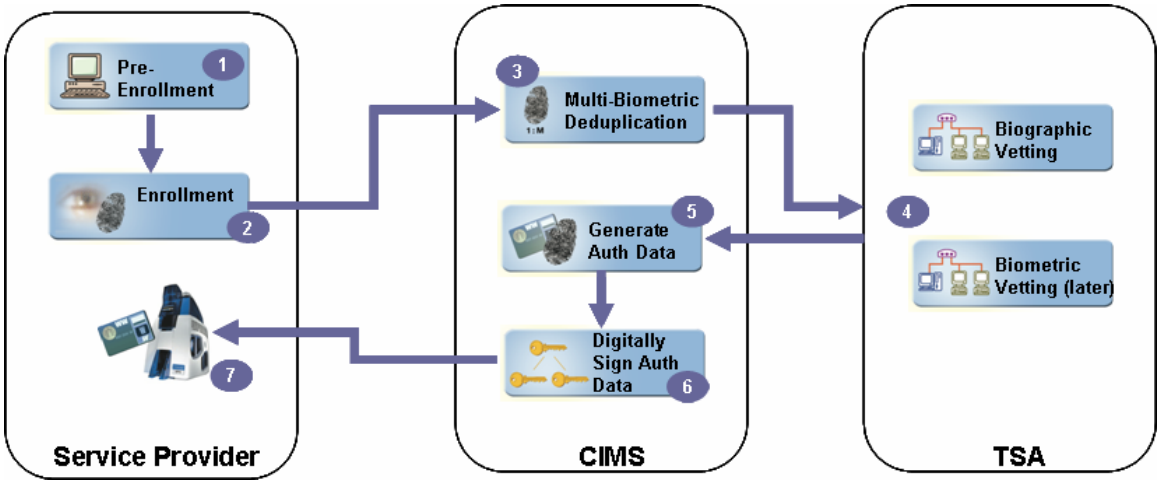


Figure 2-1. Basic Enrollment Process

The following summarizes the steps outlined in Figure 2-1 above:

1. The RT Applicant provides biographic data at (optional) pre-enrollment phase.
2. Service Provider collects biometric data and forwards enrollment record to the CIMS.
3. The CIMS receives enrollment data, performs quality checks, multi-biometric duplicate checks.
4. The CIMS provides data to the TSA vetting gateway. The TSA performs vetting.
5. On successful vetting, the CIMS generates card authentication data from enrollment data.
6. The CIMS digital signs the authentication data to prevent tampering at returns to Service Provider.
7. The Service Provider produces the smart card and provides to the RT Participant.

An RT Applicant provides biographic information, such as name, date of birth, address, and driver's license number (with state of issuance). The RT Applicant must also provide biometric information, allowing their fingerprints and facial image to be captured, as well as optionally their iris images. At the time that the biometric information is captured, the RT Applicant must also provide a set of required documents for identification purposes. The combination of biographic and biometric information constitutes the core enrollment application, which is processed by the EP, the Central Information Management System, and the Transportation Security Administration.

The CIMS acts as an information and process broker in the enrollment process, centralizing TSA clearance requests/responses, biometric duplicate checks, and TSA fee collection, as well as generating the biometric authentication data to be used for confirming an individual is a legitimate RT Participant at the verification stations. Once the CIMS receives the enrollment package, a biometric duplicate check is performed by checking the enrollment biometrics against the biometrics of other RT Participants. If there are any matches, the TSA performs adjudication to determine if this is simply another record for the same person, or if this is a fraudulent attempt to obtain an RT card under a false identity.

The CIMS passes the enrollment package to the TSA for a Security Threat Assessment (STA). Presuming that the TSA clears the Applicant for participation in the RT program, the TSA returns an acceptance message to the CIMS. Once this is received, the CIMS builds an authentication payload (including the biometric information to be used for verification), which is digitally signed and returned to the EP. Once the EP acknowledges receipt of the authentication payload, the CIMS deletes biographic information from its own databases, thereby reducing the risk of compromising personal identity information.

Finally, the EP creates an RT card containing the authentication payload as well as EP-specific information. The EP delivers the RT card to the RT Participant.

2.1.2 Overview of RT Verification Process

Biometric verification of RT Participants is a key feature of the RT program. Biometric technology will be used to confirm that the holder of an RT card is the person to whom the card was issued. A biometric presented at the verification station must be matched to the biometric information contained in the RT card in order to ensure the integrity of the RT program.

Manual verification of RT Participants (such as permitting holders of the card to pass through the RT line based on name, photo, or simple possession of the RT card) will not be allowed; indeed, the TSA requires that the RT card carry a specific disclaimer that the RT card is not valid US Government identification and that penalties may be levied for fraudulent or unauthorized use.

Although there are exceptions and alternate functions (detailed in Section 2.4, RT Use Cases), the following figure serves to illustrate the processes involved in basic RT verification:

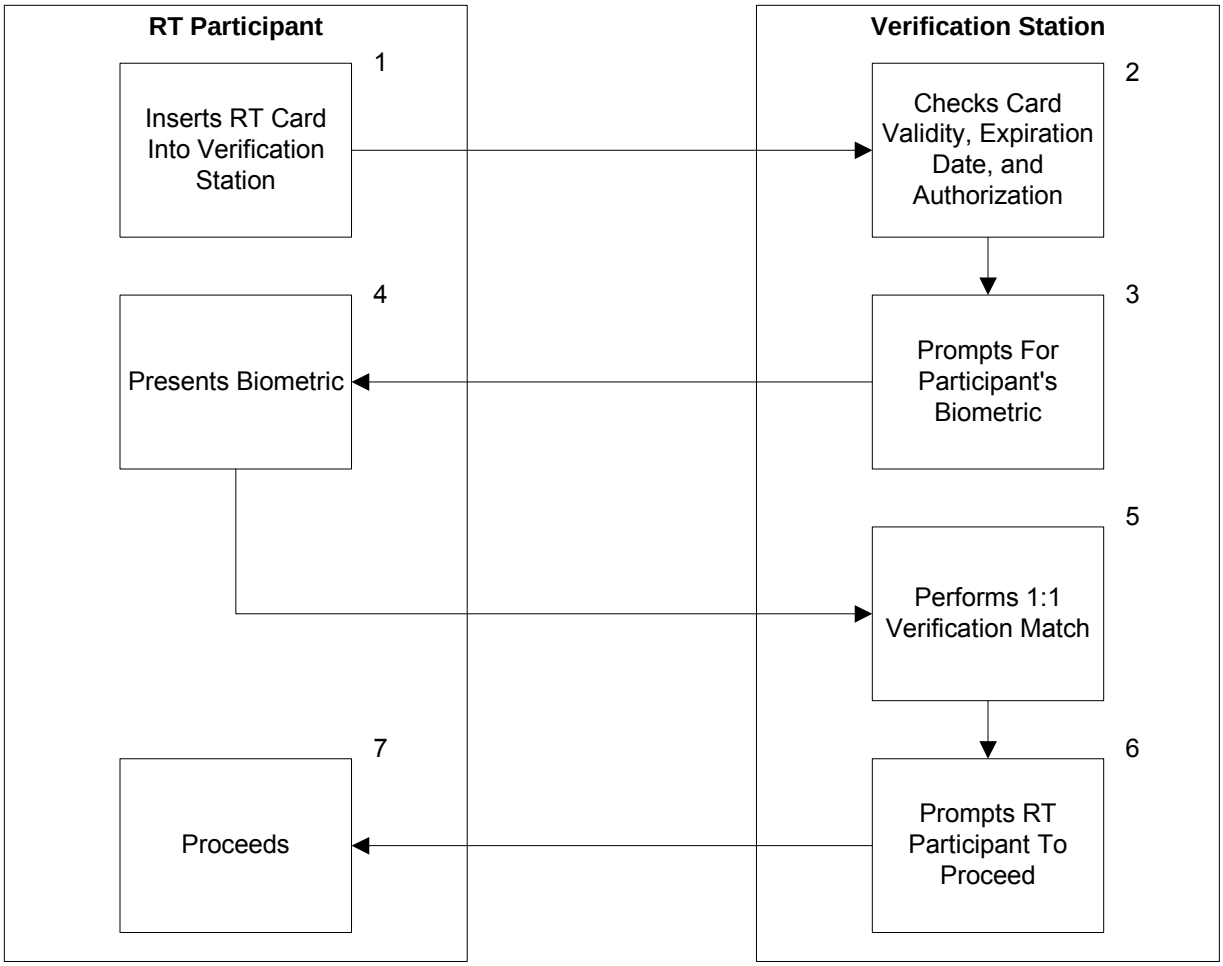


Figure 2-2. Basic Verification Process

1. The RT Participant presents their RT card at the verification station.
2. The verification station checks that the RT card is valid (through mutual authentication and digital signatures on the data), hasn't expired (based on expiration date), and is authorized (card not on the CRL).
3. The verification station prompts the RT Participant to present a biometric for capture.
4. The RT Participant presents their biometric to an appropriate biometric capture device (e.g., fingerprint scanner).
5. The verification station captures the biometric and performs a 1:1 biometric match between this biometric information and the biometric information read from the RT card.

6. The verification station prompts the RT Participant to proceed through the RT lane.

7. The RT Participant proceeds through the RT lane to the next step in the security checkpoint process.

The verification station must be capable of reading the RT card and biometric authentication data contained in the RT cards issued by all EPs. A Verification Provider is responsible for the timely update of interoperable system data (e.g., encryption keys) and CRLs, as detailed in Section 6, System Security, and Section 2.3.5.6, Revocation Process.

2.2 RT Participants

2.2.1 Participant Enumeration

There are several associated identification numbers that are used in the issuance of an RT card. Most fundamental are those identifiers that specify an individual, as well as an individual card. This hierarchy of identification numbers must be defined in order to facilitate a discussion of the architecture of the RT program. The following diagram illustrates the relationships between the various identifiers:

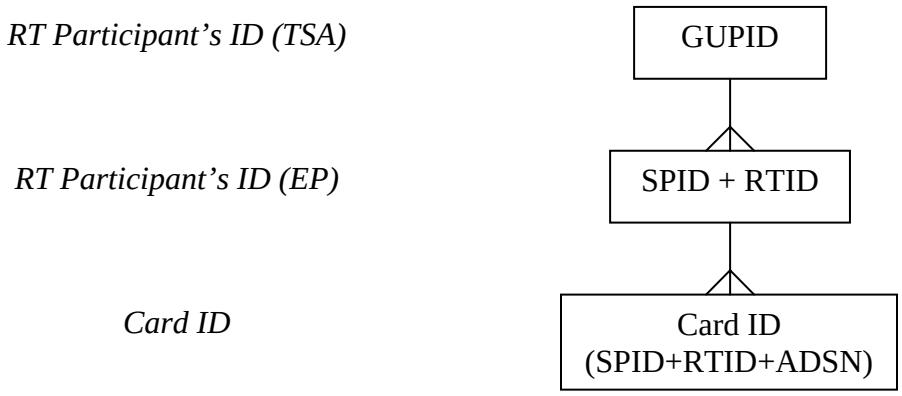


Figure 2-3. Hierarchy of Identifiers

- GUPID: RT Participant's ID, maintained by the TSA, and unique for a given individual.
- SPID + RTID: RT Participant's ID, maintained by each EP. This number is the identifier of the EP (SPID) plus identifier of the RT Participant defined by the EP (the RTID). Together, these are unique to a Participant.
- Card ID: an ID that is unique to a card, rather than an individual, through the use of an incrementing Authentication Data Sequence Number (ADSN).

GUPID. The TSA maintains a case file on each individual who has applied for the RT program, using a Globally Unique Personal Identifier (GUPID). Regardless of whether the RT Applicant is accepted or declined, or how many different RT cards have been issued to the RT Participant from various EPs, the TSA will associate all eligibility-related information with a single GUPID for a given individual.

SPID + RTID. An RT Participant may subscribe to multiple EPs. When an RT Participant subscribes to the RT program through an EP, that EP assigns its own RTID to the RT Participant. RTIDs may not be

unique between EPs, since different EPs could use the same number to represent different people. However, the CIMS assigns identification numbers to EPs and VPs known as Service Provider Identifiers (SPID). The combination of a SPID and RTID will be unique, since the RTID must be unique for a given SPID. For each RT Participant, the CIMS is responsible for maintaining the association between the RT Participant's unique GUPID and potentially multiple SPID/RTID combinations.

Card ID. If a card is lost or stolen, it will be necessary to revoke the original card and issue a new card. To facilitate the revocation of an individual card rather than an entire account, an additional identification is required that represents a card sequence number – the ADSN. This sequence number is in no way associated with the specific serial number of the card. It is simply used to keep each card's payload unique, so that a stolen card may be specifically revoked without affecting the new card that was issued to replace it. The Card ID consists of the SPID, RTID, and ADSN, as shown in the following figure:

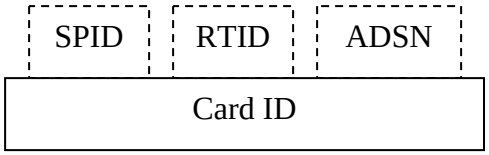


Figure 2-4. Composition of the Card ID

The ADSN is incremented each time that a new card is issued to an RT Participant (for a given EP), resulting in a new Card ID. This allows an RT Participant to maintain a single identification number with an EP (the RTID), while allowing specific cards to be revoked (using the Card ID).

2.2.2 Participant Categories

Four distinct groups of individuals are defined for participation in the RT program (though this may be expanded in the future):

- RT participants
- SP officers
- SP employees
- RT Pilot Participant or others who have been pre-approved by TSA for submittal without the initial RT fee

These groupings determine to some extent how the associated records are processed (see section 2.6.) It is possible for an individual to be in more than one participant category.

2.3 Transportation Security Clearinghouse

2.3.1 Overview

The AAAE's Transportation Security Clearinghouse acts as a trusted agent of the TSA and performs several functions important to security and interoperability. The TSC manages the CIMS, which performs the following functions:

- Accepts enrollment data from the EPs.

- Performs biometric duplicate checks on the enrollment data.
- Forwards enrollment data to the TSA for the TSA's Security Threat Assessment (STA).
- Forwards payments from EPs to the TSA for the government vetting services.
- Passes the results of the TSA's STA to the EP.
- Maintains association between individual's unique GUPID and multiple SPID/RTID combinations (one per EP)
- Generates an authentication payload for RT Participants which is sent to the EP (the EP in turn encodes the authentication payload into the RT card).
- Maintains and distributes the Card Revocation List (CRL). The TSA is responsible for informing the CIMS of the STA status of RT Participants on a perpetual basis, while the EPs are responsible for informing the CIMS of any lost, stolen or revoked cards as well as cancelled RT Participants' accounts (e.g., due to cancellation or expiration). Any cards that are no longer authorized for RT use (through TSA determination, card loss, or program cancellation) are added to the CRL.
- Stores and maintains biometric data indefinitely

2.3.2 Functional Diagram

Figure 2-5 illustrates the functional flow of the overall RT program. It includes the following steps: The EP collects biographic and biometric information from an RT Applicant and transmits it to the CIMS (Steps 1 and 2). The CIMS formats and transmits the data to the TSA (Step 3). The TSA conducts a Security Threat Assessment at application and re-vets on a perpetual basis (Step 4) and transmits an approved or not approved finding back to the CIMS (Step 5). The CIMS informs the EP of acceptance or non-acceptance (Step 6), and the EP informs the RT Applicant and issues a card with the authentication payload created at the CIMS if he or she is approved (Step 7). When an RT Participant travels through a participating airport, they use the RT card at an RT verification station which confirms the individual's current status in the RT program (Step 8).

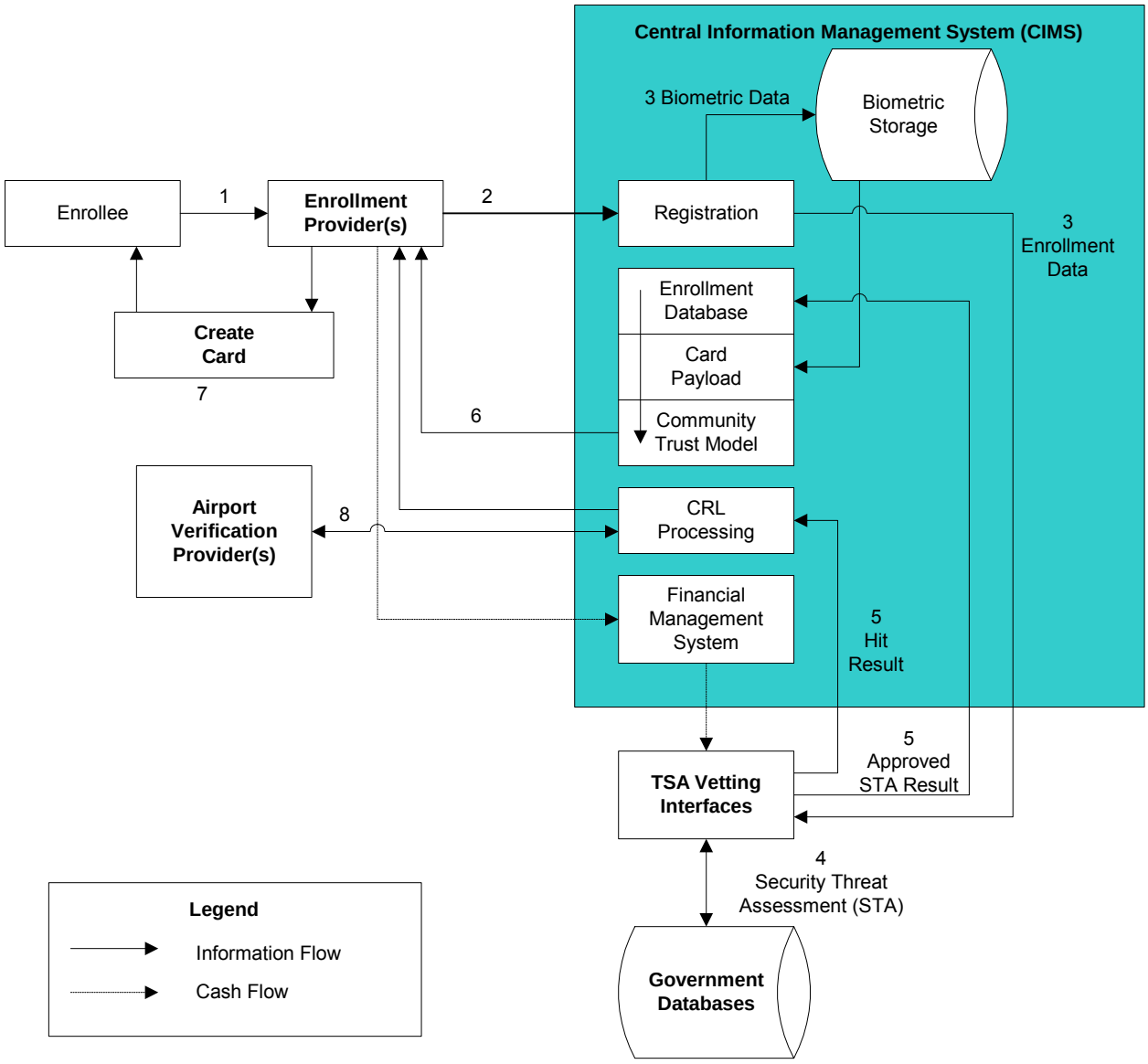


Figure 2-5. Functional Flow of the RT Program

2.3.3 CIMS Data Model

The CIMS does not maintain biographic information after the vetting by TSA is complete, thereby reducing the risk of compromising personal identity information. It does maintain identification numbers (i.e., GUPID, SPID/RTID, Card ID), as described above. The following table illustrates the type of data that CIMS will maintain on individuals (identifier values are for example only):

	Payload ID (Card ID + Expiration Date)			
GUPID	**SPID**	**RTID**	**ADSN**	**Expiry Date**
123456789	AC	1234ABCD5678EF90	A	20051231
123456789	AC	1234ABCD5678EF90	B	20101231
123456789	MA	CBCCRC_1246ENEDC	A	20091231
987654321	AC	ABCD_1234_OSAIOR	A	20101231

Figure 2-6. Example CIMS Data for RT Participants

In this table, the individual with a GUPID of 123456789 is associated with three cards, and the individual with a GUPID of 987654321 is associated with a single card. The first individual is/was enrolled with EP AC or "Acme" (where he was assigned an RTID of 1234ABCD5678EF90) and EP MA or "Malta" (where he was assigned an RTID of CBCCRC_1246ENEDC). This individual had two cards with Acme, differentiated by different ADSNs, which translate to different Payload IDs. Although it is possible to briefly have two active cards (if the two cards are in a brief overlap window while the EP is issuing a new card), in this example the first card is not active since it expired on 12/31/2005.

The CIMS also maintains biometric information in order to facilitate biometric duplicate searches. When an RT Applicant first enrolls with an EP, their biometric information is sent to CIMS for comparison with the biometric data maintained by CIMS (see Section 2.3.5.1, Biometric Duplicate Resolution, for more information). Biometric duplicate searches are done in order to determine if a) the individual already exists in the database as a legitimate RT Applicant with a pre-existing GUPID, or b) the individual already exists in the database under a different identity and may be attempting a fraudulent application. Biometric data is associated with the unique combination of SPID and RTID (identifier values are for example only and are not representative of actual syntax or content):

SPID	RTID	Biometric Data
AC	ABCD1234EFGH5678	<Biometric01>
MA	IJK9876CBC3340DC	<Biometric02>

Figure 2-7. CIMS Biometric Data

When an enrollment package is first received, the CIMS has both biographic and biometric information. Once the application has been approved by the TSA and the authentication payload has been received and acknowledged by the EP, the biographic information is deleted. The CIMS also deletes the facial image and the scanned identity documents at this time. Since the information that is deleted (biographic information, facial information, scanned documents) is not required for further CIMS functionality, deleting this information reduces the risk of loss of personal identity information.

In the example shown in Figure 2-7, if the RT Applicant initially applies with Acme (and has never applied to the program before), the biometric duplicate check should result in a "no match" and the associated

biographic data purged upon completion of the process (e.g., once the authentication payload has been accepted by the EP).

However, if the same RT Applicant subsequently applies with Malta, then the biometrics provided by Malta should result in a match during the duplicate check. To adjudicate that match (i.e., determine if the match is legitimate, with the biographic information being consistent between the two applications, or fraudulent, with different identities associated with the same biometrics) the biographic data from Acme must be compared against the biographic data from Malta. Such adjudication is performed by the TSA, which maintains biographic information on all RT Participants. Therefore, if a biometric match is found, the CIMS forwards the application as well as information associated with the matches to the TSA through the TSA Vetting Interfaces.

2.3.4 Important CIMS Requirements

There are a number of important requirements that pertain to the CIMS that may not be explicitly covered in the following use cases, such as data retention and data storage requirements. These include:

- The CIMS shall not retain the RT Participants' biographic information, facial image, or scanned identity document information once the biometric payload is accepted by the EP.
- The CIMS shall retain standard biometric and identification data indefinitely for RT Participants revoked by the TSA.
- The CIMS shall maintain the CRL, combining revocation requests from the TSA and individual EPs.
- The CIMS will store biometric data (possibly as part of an offline storage archive) in accordance with the records retention requirements of the National Archives and Records Administration (NARA).

2.3.5 CIMS Processes

2.3.5.1 Biometric Duplicate Resolution

When an individual applies to the RT program through an EP, part of the initial enrollment package that is sent to the CIMS is the RT Applicant's biometric information. This biometric record is checked against all of the records in the CIMS biometric database (1:N search). The records in the CIMS biometric database include:

- All current RT Participants
- Previous RT Participants who were revoked by the TSA
- Previous RT Participants whose participation ended
- RT Applicants who applied to the RT program but were rejected by the TSA.

There are a number of reasons to check for biometric duplicates:

- If the RT Applicant is already in the system with a different EP, then it is important to associate the current application with the previous GUPID that is already known by the TSA.
- If the individual is already known in the system, but under a different name, then there is the potential that this is a fraudulent application.

The purpose of duplicate resolution is simply to determine whether the biometric match was legitimate (same name/address, such that it appears to clearly be the same person) or fraudulent (biographic information is different enough to suspect that the application might be an attempt to fraudulently obtain an RT card under a different alias).

When an enrollment package is received from an EP, the CIMS performs a biometric duplicate check against the biometric database. Each biometric is compared against the CIMS biometric database. If the comparison of one of the RT Applicant's biometrics to any biometric in the database results in a comparison score above a certain threshold, then this is a potential match. The CIMS takes potential matches and performs biometric hit confirmation, potentially using other biometrics on record.

Once a biometric match has been confirmed, the CIMS forwards the application as well as information on all potential matches to the TSA. Since the TSA maintains all biographic information and has personnel trained in duplicate adjudication, the TSA compares the biographic information of the application against the biographic information associated with the biometric matches. The results of this adjudication are returned to the CIMS.

The TSA will also perform a STA on applications returned from a biometric duplicate resolution. If the TSA determines that the application did not match any of the potential matches, then the Applicant will be assessed as a new record in the system. If the TSA determines that the application did match an existing record in the system, then the STA will incorporate information from the application into the whole record when considering the STA. Presumably, if the application was potentially fraudulent (i.e., an attempt to apply under a false identity) then the STA would be reject the application.

Note, the actual message implementation may differ slightly as the TSA Vetting Interfaces are defined.

2.3.5.2 Enrollment Packaging

The initial enrollment package sent from the EP to the CIMS includes all biographic and biometric information and scanned documents. As discussed above, the CIMS performs a biometric duplicate check and forwards the application (if there was no fraud detected) to the TSA for an STA. Once the TSA has approved the application, the CIMS builds an authentication payload for the EP to include on the RT card.

As discussed in Section 2.2, RT Participant Enumeration, the Card ID uniquely identifies the card through the combination of the SPID, RTID, and ADSN. However, as noted earlier, the CIMS actually stores the Payload ID, which is comprised of the Card ID and the expiration date of that specific card, as illustrated below:

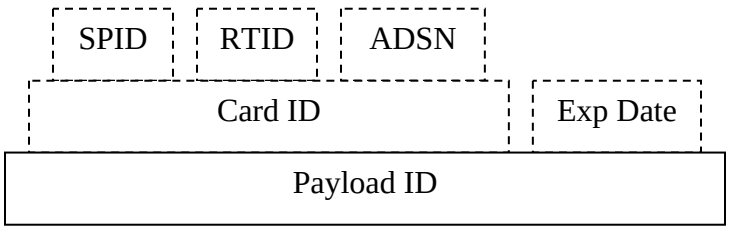


Figure 2-8. Composition of the Payload ID

The expiration date allows the CIMS to determine when a card revoked by an EP may be removed from the CRL (as discussed in Section 2.3.5.6, Revocation Process). As shown in the following figures, the Payload ID is the identifier that is used to tie the CIMS' biometric data to additional EP-data on the RT card.

Once an RT Applicant has been approved by the TSA, the CIMS builds a digitally signed authentication payload to be placed on the RT card by the EP. Due to the inclusion of the ADSN in the Payload ID, the authentication payload is unique for each card. The authentication payload includes processed biometric data (such as fingerprint templates, facial image, and iris images) derived from the biometric information sent to the TSA for the STA. The authentication payload is digitally signed by the CIMS and consists of this biometric data combined with the Payload ID identifier, as shown below:

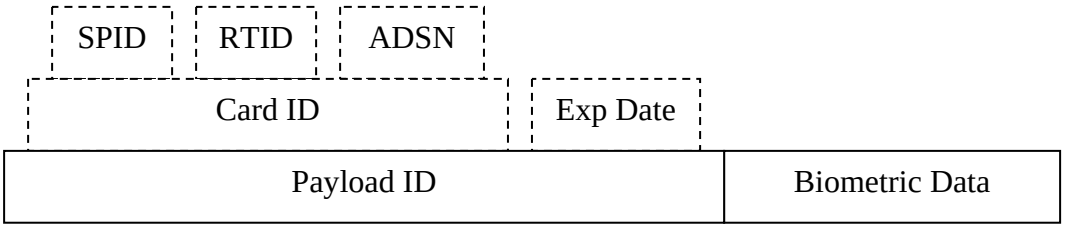


Figure 2-9. CIMS Authentication Payload

Once the authentication payload is created, it is sent to the EP for inclusion on the RT card. However, the EP has its own data to place on the card: the card-specific payload. As mentioned earlier, the card-specific payload is associated with the authentication payload through the use of the Payload ID, which is common to both payloads.

The card-specific payload includes the Verification ID (VID), discussed below, as well as other non-RT EP-specific data, such as EP-specific benefit information (e.g., preferred parking or car rental information). The EP combines the Payload ID with the VID to form a Registered Traveler Unique Identifier (RTUID). The RTUID is, in turn, combined with the EP-specific data to form the card-specific payload, as shown below:

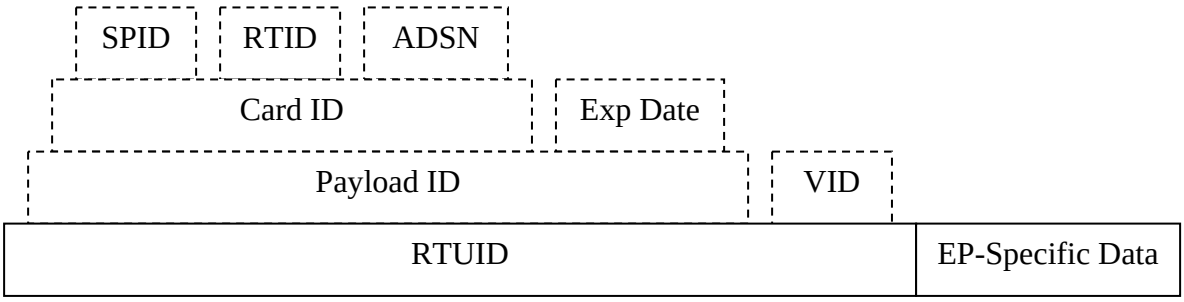


Figure 2-10. Card-Specific Payload

When the authentication payload is received from the CIMS, the CIMS-signed Payload ID is combined with the VID to form the RTUID. This is then signed by the EP and placed on the card along with the

CIMS-signed biometric information and the EP-specific data. The inclusion of the unique Payload ID as part of both the authentication payload and the card-specific payload allows these two objects to be verifiably associated. The use of CIMS-signed data for the Payload ID and the biometric information provides a chain of trust back to the CIMS. The use of mutual authentication between the card and the card reader (discussed in the Verification Use Case) prevents the biometric data from being copied (or even read) by unauthorized personnel.

The purpose of the VID is to allow an EP to optionally assign a unique anonymous ID to the user for billing purposes. In order to prevent tracking of RT Participants, the RTID of the RT Participant is not recorded at the verification station (except under exceptional conditions such as when the RT Participant's authorization has been revoked by the TSA). However, an EP should be able to request a bill from a VP for verification transactions that includes some sort of identifier for each card. This would be for auditing purposes, to ensure that the verification transactions involve unexpired cards that were issued by that EP.

Each EP may elect not to use the VID to differentiate between cards or to use the VID to anonymously differentiate between cards. For example:

- An EP may choose to populate all of its cards with VIDs that have the same value, effectively nullifying the usefulness of the VID as a unique card identifier. This would restrict tracking information being stored for individual cards, but would also prevent the ability to present unique card transactions when billing that EP.
- Another EP may choose to put a unique but anonymous ID in the VID, with no association to the individual's identity; this would allow the EP to accept bills from VPs containing unique VIDs.

Regardless of whether an EP chooses to associate unique numbers with each VID, the EP must not retain the VID in any association with the RTID. By business policy, an SP (either EP or VP) is not allowed to record the association of RTID and VID; it exists only on the card. An EP may record the VID along with the expiration date as a means to validate that a card was generated with that ID, and a VP may record location and date/time information associated with the VID at the time of a verification transaction. However, neither the EP nor the VP may associate the VID with the traveler's identity.

2.3.5.3 Card Re-issuance Process

There are circumstances under which an EP will need to re-issue an RT card to an RT Participant. For example, if the RT Participant's card is lost or stolen, a new card will have to be created and issued. When a new card is issued, the lost, stolen, or damaged card is revoked.

However, a 14 day grace period can be used when issuing a new card if the original card is still usable. During this time, the original card is still operational. This allows a new card to be shipped to the RT Participant, while still allowing the current card to be used in the interim. For instance, if an RT Participant reports that his card is only working intermittently, a new card can be produced and shipped while the RT Participant continues to make do with his existing card.

As noted earlier, the CIMS maintains the biometric information; therefore, the CIMS can rebuild the authentication payload on request. The EP simply requests that CIMS send a new authentication payload for a given RTID by sending the current card's Card ID:

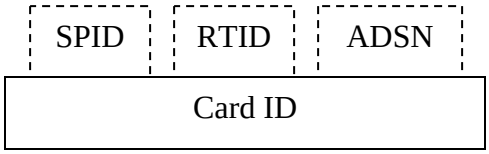


Figure 2-11. Re-issuance Request Format

When the CIMS receives this request, it first verifies that the requested RTID is associated with the requesting EP. The CIMS then builds a new authentication payload. The principal difference between the new authentication payload and the old authentication payload is that the ADSN is incremented for uniqueness, resulting in a new Card ID. The signed authentication payload is then sent back to the EP for use in the issuance of a new card.

Whenever the CIMS receives a re-issuance request, CIMS automatically starts a 14 day timer on the original card. At the end of this time period, CIMS will automatically revoke the original card. If the EP is required to immediately revoke the original card (e.g., card is known to be lost, stolen, or destroyed), then the EP must send a separate revoke message to explicitly revoke the original card, thereby stopping the 14 day grace period on the card and revoking it immediately.

2.3.5.4 Re-enrollment Process

Re-enrollment, primarily re-capturing biometric information, is separate from card re-issuance. Re-enrollment will be necessary in certain circumstances, such as when an RT Participant does not renew their participation but decides at a later date to rejoin the program. In addition, the TSA will require periodic re-enrollment of all RT Participants. The TSA is still formulating the guidelines for re-enrollment but requirements pertaining to re-enrollment will deal with:

- Frequency. Re-enrollment must occur every five years as defined by the TSA.
- Biometric re-enrollment, policies, and practices.
- Identity source document re-vetting.
- Submission of updated biographic information to the TSA. This is discussed in Section 2.3.5.5, Biographic Update Process. It is not anticipated that biographic updates will require re-enrollment.

If the RT Participant wishes to update their biometric information, then the RT Participant must re-enroll and a new card must be issued. For instance, if the RT Participant changes their mind about iris enrollment, or wishes to use a finger that was bandaged at the time of initial enrollment, then a full re-enrollment must occur. Biometric re-enrollment might also be necessary if the RT Participant is failing biometric verification with some frequency.

2.3.5.5 Biographic Update Process

EPs must advise RT Participants to update their biographic information within 30 days of any changes occurring. Otherwise, RT Participants may volunteer changes to their biographic information at any time. At a minimum, EPs are required to report an update from RT Participants. The update request should provide current biographic information, and should provide the ability for the RT Participant to provide updates to biographic information.

Many biographic fields may be updated by the RT Participant in an unsupervised manner (e.g., via paper form, or online). Updates to some major biographic fields (e.g., last name, first name, gender, DOB), to be specified by the TSA, will require verification with the EP using updated identity source documents. Any updates that are made to an RT Participant's biographic data are passed to the TSA at least annually through the CIMS for use in the TSA's ongoing STA process.

2.3.5.6 Revocation Process

Owners of valid, unexpired RT cards are authorized to utilize RT benefits unless they are specifically excluded via a list of revoked cards, a Card Revocation List. The CRL is maintained within the CIMS, and is provided to VPs on a regular basis (every 12 hours) or upon request.

VPs are responsible for propagating CRLs received from the CIMS to all of their verification stations. It is anticipated that such propagation should only take minutes; however, it is required to occur within six hours of receipt from the CIMS to accommodate airport operations and offline verification stations. If a verification station has not received an update from the CIMS within 24 hours, it must cease to accept RT Participant verification requests, since the station may not have the latest CRL.

The CRL specifies all revoked cards, including cards revoked by either the issuing EP or the TSA. It is anticipated that the CRL will be updated often, as EP subscriptions naturally expire or cards are reported lost. Less frequently, the TSA will revoke an existing RT Participant through its ongoing STA.

Every 12 hours, the CIMS will push the current CRL to all VPs (full CRL). On an as needed basis (e.g., the TSA revokes someone and specifies that this person must be revoked immediately), the CIMS will push updates to the VPs that contain only the cards that have been revoked since the last push of the full list (partial CRL).

For example, the CIMS pushes a complete CRL to all VPs at 1:00. At 9:00, the CIMS receives an addition to the CRL that requires immediate distribution to the VPs and pushes an update that contains only the cards that have been revoked since 1:00. At 9:30, the CIMS receives another addition to the CRL that requires immediate distribution to the VPs and sends out a second update that contains all of the cards that have been revoked since 1:00. This update replaces the previous update, and does not represent an update since the last update. Each update represents a complete list of cards that have been revoked since the last push of the complete list.

Although VPs should always have the latest distributed CRL sent by the CIMS, VPs may also request CRL download. This might be necessary if the VP has been offline for any period of time and is unsure if its CRL is current. To do this, the VP sends a CRL request message to the CIMS that contains the identifier of the latest CRL update. The CIMS may then respond indicating that no update is required (i.e., the VP has the latest list), that an update is required (and include the update), or that a full CRL list was missed (and include the latest full CRL).

The CRL (full or partial) will include a CRL expiration date/time (24 hours from creation). VP kiosks will use this to determine if the CRL it has is valid. If that CRL's expiration has passed, the kiosk must cease operation until a new CRL is received (as described above). If the kiosk has a consolidated CRL (a full CRL combined with a partial CRL/update, the expiration date on the partial CRL will be used as the expiration date of the combined CRL.

There are four types of revocation requests:

1. Revoke all cards issued by a given EP.
2. Revoke all cards issued to an RT Participant (regardless of EP).

3. Revoke all cards issued to an RT Participant by a specific EP.
4. Revoke a specific card.

The following table describes these requests, as well as who may request each type of revocation and what type of data is used to perform the revocation:

Type of Revocation Request	Requesting Entity	Values Used In Request			
		GUPID	SPID	RTID	ADSN
EP level. Revoke all cards issued by an EP.	TSA		X		
RT Participant level. Revoke all cards issued to an RT Participant regardless of EP.	TSA	X			
RT Participant level (for one EP). Revoke all cards issued to an RT Participant by the requesting EP.	EP		X	X	
Card level. Revoke a specific RT card that was issued by the EP.	EP		X	X	X

Table 2-1. Types of Revocation Requests

EP Level - The TSA may request that all cards issued by an EP be revoked. This could occur if the EP goes out of business, or fails to maintain conformance standards in some way. The CIMS is responsible for ensuring that all of the unique Card IDs associated with the EP are placed on the CRL. This will be accomplished by the use of a special “EP Revocation” entry in the CRL that includes only the SPID. Each VP must ensure that any cards associated with that EP are not honored.

RT Participant Level - The TSA may also request that all cards issued to an RT Participant be revoked. This is likely to occur as a result of the TSA’s ongoing STA process. If at some point the TSA determines that an individual’s STA no longer warrants participation in the RT program, then it must ensure that all cards issued to that person, regardless of EP, get revoked. The TSA sends the RT Participant’s unique GUPID to the CIMS, and the CIMS is responsible for first determining the EPs with which the individual is enrolled (SPID), and then the RTID of the individual with each EP. Once again, the CIMS is responsible for ensuring that all of the unique Card IDs associated with the individual are placed on the CRL. This will be accomplished by the use of a special “RT Participant Revocation” entry that includes only the SPID + RTID. Each VP must ensure that any cards associated with that SPID+RTID are not honored.

RT Participant Level (For One EP) - An EP may request that all of the cards it has issued to an RT Participant be revoked. This is likely to occur if the RT Participant fails to renew their subscription through the EP. The EP sends its SPID as well as the RT Participant’s RTID to CIMS, which is responsible for using the special “RT Participant” entry noted above. Each VP would ensure that any cards associated with that SPIC + RTID are not honored.

If an EP revokes an RT Participant and that RT Participant has no active cards with any other EP, then the CIMS must notify the TSA of the revocation. The TSA wishes to know when an individual is no longer participating in the RT program so that it can cease the ongoing STA for that person.

Card Level - An EP may also request that a specific card issued by the EP to the RT Participant be revoked. This is likely to occur if the RT Participant reports the card lost, stolen, or damaged. The EP sends the specific Card ID to the CIMS, which places the Card ID on the CRL.

For all of the different types of revocation, it is also possible for the requesting entity to suspend instead of revoke. The only difference between revocation and suspension is that suspended cards may be removed from the CRL at the request of the requesting entity. Caution must be used in implementing the logic of lifting suspension, however, to ensure that if a card is suspended/revoked by both the EP and the TSA, that a request to lift the suspension by only one entity does not automatically reactivate the card.

The general idea of the CRL is that only unexpired cards need to be retained in the CRL. Once a card expires, it may be removed from the CRL. Since the expiration date is in the card and digitally signed by the CIMS, the expiration will prevent the card from being used; therefore, it is safe to remove the card from the CRL and still maintain the expectation that the card cannot be used. However, the TSA would like to maintain a record of attempts to use cards that were revoked by the TSA, regardless of whether the card itself is expired. For this reason, it will be necessary to maintain TSA-revoked cards on the CRL even after those cards have naturally expired.

2.4 RT Use Cases

The following use cases describe the processes and requirements associated with several of the major RT functions.

2.4.1 Enrollment

The following use case outlines the steps involved in the enrollment of an RT Applicant into the RT program, including the typical enrollment flow, as well as biometric duplicate resolution, association with existing records, and rejected applications. In Figure 2-12, Enrollment (1 of 3), the first five actions represented may vary in sequence based on EP implementation (however, the verification of the EP Enrollment Officer must be the first action performed).

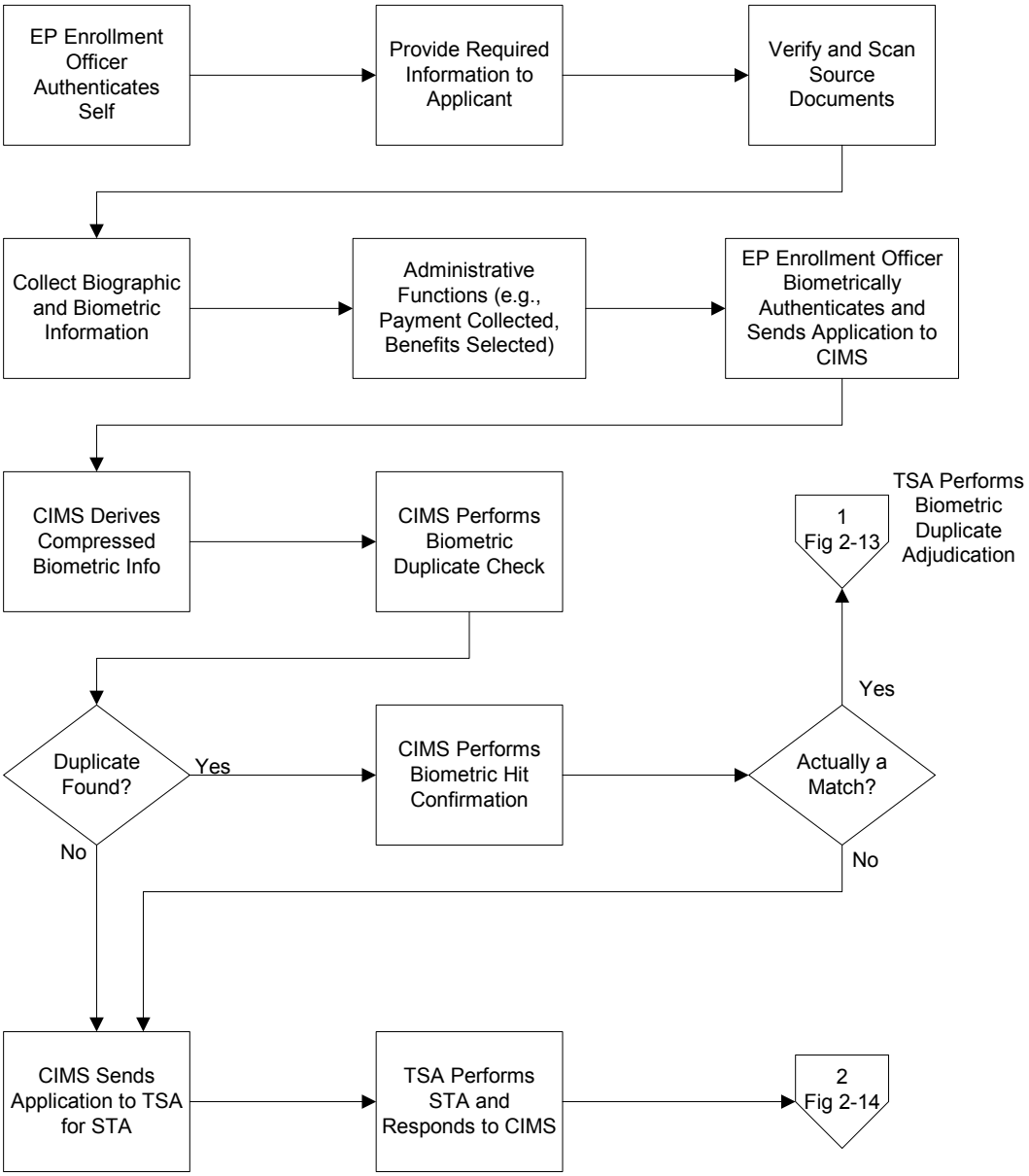


Figure 2-12. Enrollment Process (1 of 3)

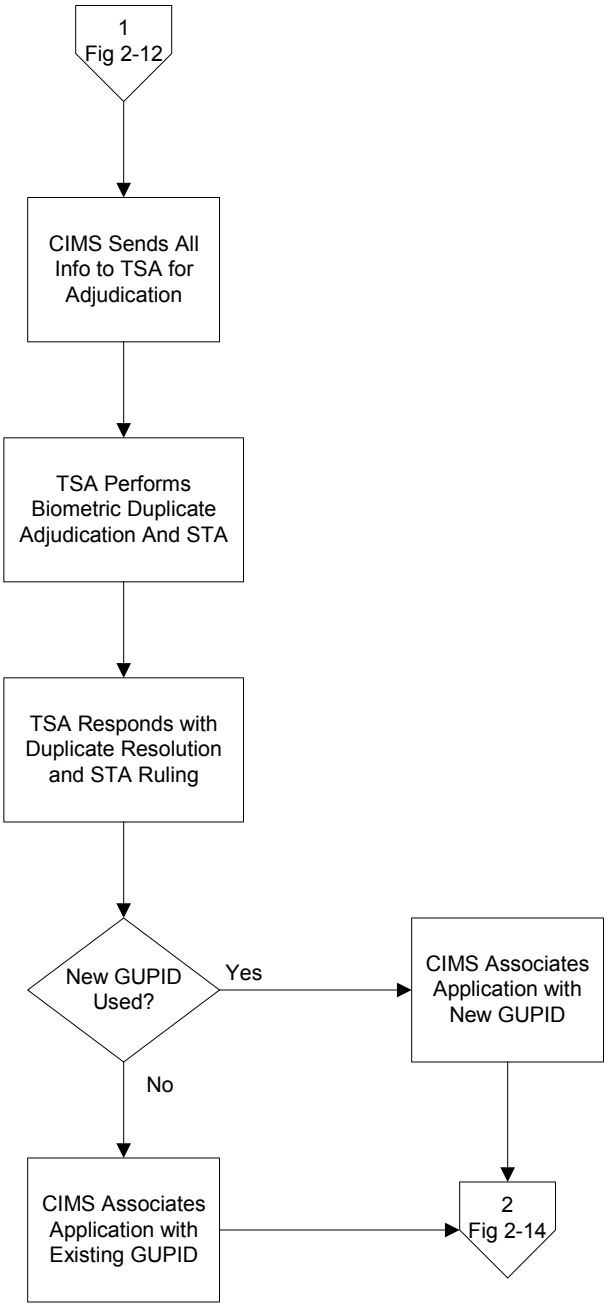


Figure 2-13. Enrollment Process (2 of 3)

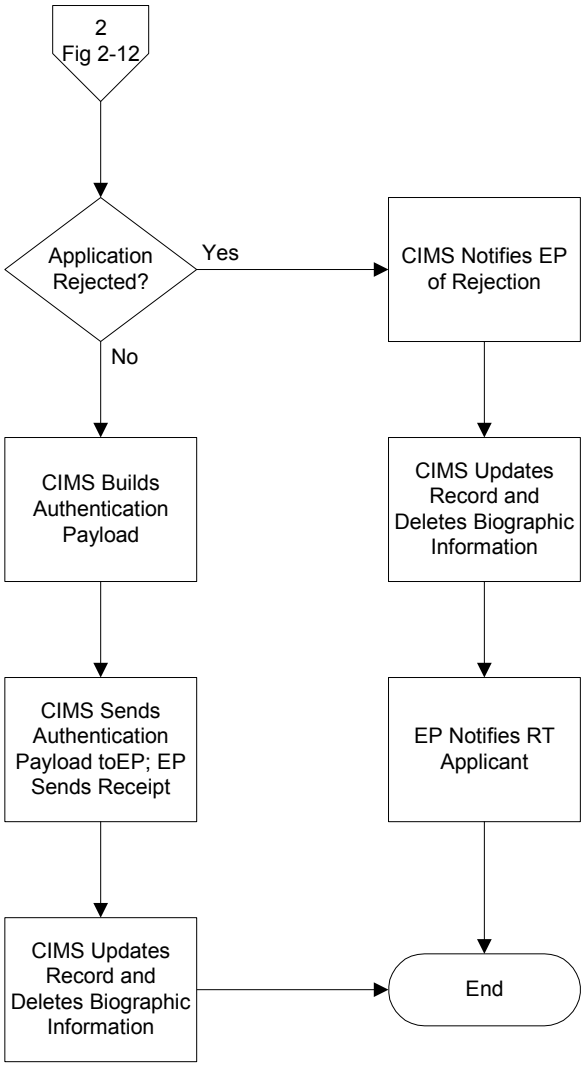


Figure 2-14. Enrollment Process (3 of 3)

Main Flow

The following process outlines the steps involved in a typical enrollment (steps 2-5 may vary in sequence based on EP implementation, other than EP Enrollment Officer verification occurring prior to document vetting and biometric collection):

1. EP Enrollment Officer authenticates with the enrollment station for this particular enrollment.

2. EP provides required information to RT Applicant (e.g., EP privacy information, EP Terms & Conditions, TSA Terms & Conditions, RT program information (e.g., interoperability options)).

3. EP performs ID document vetting, including scanning documents and collecting electronic identity document information from the RT Applicant where applicable. This also includes verifying RT Applicant-supplied biographic information against the identity source documents. The TSA will provide guidance on processing multiple source documents with conflicting data (e.g., name spelled differently on different documents).

4. EP collects components of enrollment package. This includes all required biographic information (e.g., name, DOB, address, and identification information), scanned and electronic identity document information, biometric information (e.g., facial, fingerprint, and iris images (optionally)) that satisfy quality requirements, and biometric preferences. Biographic information may be collected in advance via the Internet. Refer to the requirements subsection in this use case for requirements pertaining to data that must be collected.

5. EP performs administrative functions (e.g., collecting payment information, enrolling in vendor-specific benefit programs, assigning an EP-unique RTID). Administrative information may be collected in advance via the Internet.

6. EP Enrollment Officer authenticates with the enrollment station for this particular enrollment to "sign" the enrollment package.

7. EP sends RT Applicant's enrollment package to the CIMS.

8. CIMS creates processed biometric information (e.g., fingerprint templates, iris image) from biometric enrollment package. This includes checking the quality of the iris images.

9. CIMS performs biometric duplicate check using biometric enrollment data. This involves fingerprints and potentially iris images.

10. If the biometric duplicate search results in a list of matching candidates, flow passes to alternate flow "Biometric Duplicate."

11. **Perform STA**. CIMS passes enrollment package to TSA for Security Threat Assessment (STA). If the TSA requires additional information in order to perform the STA, the TSA will work directly with the RT Applicant without the involvement of either the CIMS or the EP.

12. TSA returns enrollment decision.

13. **CIMS Processes STA Decision**. If TSA's enrollment decision is "Reject," flow passes to alternate flow "Enrollment Rejected."

14. Application Accepted. The CIMS builds authentication payload, consisting of Payload ID (SPID, RTID, ADSN, and Expiration Date) and biometric information (e.g., fingerprint, facial image, and iris (if supplied) information).

15. The CIMS digitally signs the authentication payload and sends to the EP. The EP sends a message to the CIMS confirming receipt of the authentication payload. The EP deletes the biometric information, unless otherwise explicitly permitted by the Applicant.

16. The CIMS updates RT record for approved RT Applicant indicating TSA approval for participation and deletes the biographic information, as well as facial image and scanned identity document information.

Alternate Flow – Biometric Duplicate

The following alternate flow describes the process by which potential biometric duplicates are resolved.

1. For every biometric match found, the CIMS first confirms that the RT Applicant biometrically matches the overall biometric record associated with the matching record. For example, the CIMS may confirm that the RT Applicant's other biometrics match the other biometrics of the matching biometric record. Biometric hit confirmation may utilize any/all other biometric information (e.g., all fingerprints and both iris images, if available).

2. If it is determined that the RT Applicant does not actually match an existing overall biometric record, then the flow returns to the main flow at "Perform STA."

3. The enrollment record is passed to the TSA for adjudication, including all information available from the CIMS (e.g., biometric and biographic information for RT Applicant and identity and biometric information for all potential matches). This also includes a new CIMS-generated GUPID, in case the biometric resolution indicates that the RT Applicant does not actually match anyone in the system and a new GUPID is required. If additional information is required in order for the TSA to perform the adjudication, the TSA will work directly with the RT Applicant without the involvement of either the CIMS or the EP.

4. The TSA performs duplicate adjudication and performs STA. Duplicate resolution involves comparing the biographic information of both the RT Applicant and each match to determine if this is the same person (e.g., applying for a second RT card, applying for the card after previously quitting the program) with the same or similar biographic information (i.e., not attempting fraud), or if it may be a fraudulent application (same person applying under a different identity). If the Applicant is not associated with any of the potential biometric matches, then the newly-generated GUPID sent by CIMS will be used for the Applicant. The TSA will also perform an STA regardless of whether this is a new GUPID or is associated with an existing GUPID.

5. The TSA responds with the biometric resolution and an STA. This informs CIMS of both the STA status of the application, as well as the appropriate GUPID (either the new GUPID generated by the CIMS or a previously existing GUPID).

6. If the response indicates that the application was not associated with a previously existing GUPID, then CIMS associates the application with the new GUPID.

7. If the response indicates that the application is associated with a previously existing GUPID, then the CIMS associates the application with the existing GUPID.

8. Flow returns to the main flow at “CIMS Processes STA Decision”.

Alternate Flow – Enrollment Rejected

The following alternate flow describes the steps by which applications that have been rejected by the TSA are processed:

1. The CIMS sends a rejection notification to the EP.

2. The CIMS updates the RT record for rejected Applicant indicating TSA rejection for participation and deletes biographic information.

3. The EP sends rejection notification to the RT Applicant, including instructions to contact the TSA if the RT Applicant wishes to appeal the decision. Any potential appeals processes are a TSA function and are outside the scope of this document. The EP deletes application information.

4. The TSA will be responsible for any enforcement action resulting from Fraudulent Matches. If a Fraudulent Match results in the revocation of a current RT Participant, the revocation request from the TSA will be placed on the CRL and handled in the same manner as all TSA revocation requests.

Enrollment Requirements

The following are a high level set of requirements that must be satisfied by the various actors within the enrollment process:

EP Requirements

1. The EP shall delete the RT Applicant’s biometric information from its own database, unless otherwise explicitly permitted by the Applicant, once the application has been approved. The request for permission must be comprehensible and concise.

2. The EP shall delete the RT Participant’s biographic and biometric information from its own database, unless otherwise explicitly permitted by the Applicant, once an application has been rejected or an existing subscription has been terminated. The request for permission must be comprehensible and concise.

3. Employees of RT Service Providers that are involved with the RT program at an airport, operate an RT component or have access to RT Applicants’ personal data shall first be vetted as required by the TSA. Depending on their job location and duties, RT Service Provider employees may also need to obtain a Security Identification Display Area (SIDA) badge.

4. The EP Enrollment Officer shall be biometrically authenticated and authorized prior to sending an RT Applicant’s enrollment package to the CIMS, so as to associate the Enrollment Officer with the vetting of documents and collection of biometrics. The responsibility for setting and modifying biometric operating parameters for Operator authentication is a conformance issue which will need to address quality control and policy issues as well as technical interoperability.

5. The EP shall ensure that the EP Enrollment Officer oversees the verification of identity source documents and the collection of biometric information.

6. The EP Enrollment Officer shall validate the RT Applicant’s identity source documents prior to submitting an enrollment package to the CIMS.

7. The EP Enrollment Officer shall verify the identity source documents using a front-end validation device or other state-of-the-art document authentication technologies that take advantage of anti-fraud features incorporated into Government-issued documents. Validation technologies shall be updated periodically to ensure conformance to the latest standards.
8. The EP shall only accept the identity source documents approved by the TSA, which will be provided in the TSA's Security, Privacy and Compliance Standards.
9. The EP Enrollment Officer shall scan the identity source documents and include such scanned images with the overall enrollment package. Future requirements may dictate that electronic document information be collected from certain documents capable of providing such information.
10. The EP shall attempt to collect biographic information in accordance with the TSA's Privacy Impact Assessment (PIA) for the Registered Traveler Interoperability Pilot.
11. The EP shall verify the captured biographic information against the biographic information on the breeder documents for accuracy. The TSA will provide guidance on processing variances between documents.
12. The EP shall collect the maximum possible of 10 flat fingerprint images.
13. The EP Enrollment Officer shall ensure that the minimum required biometric information (i.e., four fingers of sufficient quality and a facial image) has been captured prior to submitting an enrollment package to the CIMS or that a waiver is granted allowing for a minimum of 2 fingers of sufficient quality.
14. The EP shall ensure that the quality of fingerprint images satisfies the quality requirements specified in Section 3, Biometric Data Management and Use.
15. The EP shall ensure that the quality of iris images (optionally enrolled by RT Applicant) satisfies the quality requirements specified in Section 3, Biometric Data Management and Use.
16. The EP shall specify the RT Applicant's primary and secondary biometric preference. A biometric preference refers to a particular finger (e.g., right index finger, left thumb) or iris (right eye, left eye) that will be captured and used for a 1:1 biometric match during the verification process at the airport. The primary biometric preference represents the particular finger or iris that the RT Applicant desires to present at verification, while the secondary biometric preference represents the biometric to be presented if the primary preference either fails or is unavailable (e.g., the primary biometric preference is a finger which is bandaged and thus unavailable at the time of verification).
17. The EP shall provide the RT Applicant with the following information prior to submitting an enrollment package to the CIMS: EP privacy policy, Federal privacy information, EP Terms and Conditions, RT Terms and Conditions, RT program information. The TSA will provide the EP with an electronic copy of all information that is not specific to the EP.
18. The EP shall generate an RTID to assign the RT Applicant an identifier that is unique within the EP.
19. The EP shall send enrollment package applications (including biographic information, scanned identity source documents, and biometric information) to the CIMS for processing. Details of the

data format and transmission specifications can be found in the appropriate sections of this specification.

20. If an EP receives a rejected notification from the CIMS, the EP shall notify the applicant that the application was rejected, including instructions to contact the TSA if the RT Applicant wishes to appeal the decision. Any potential appeals processes are a TSA function and, as such, are outside the scope of this document.

21. The EP shall confirm receipt from the CIMS of authentication payloads.

CIMS Requirements

1. The CIMS shall maintain a biometric database of RT Applicants that includes:

    - Current RT Participants
    - TSA revoked, former RT Participants
    - Rejected RT Applicants
    - RT Participants who have terminated their subscription.

2. The CIMS shall perform a biometric duplicate check (including hit confirmation) using all fingerprint data (of sufficient quality) and potentially the iris data against a biometric database.

3. The CIMS shall generate a new GUPID for any application. For applications without biometric duplicate hits, a new GUPID must be generated for the new identity. For applications with potential biometric duplicate matches, a new GUPID must be generated in case the TSA biometric duplicate resolution indicates that there actually wasn't a match and the application is for a new individual.

4. The CIMS shall forward applications with potential biometric duplicate matches to the TSA for adjudication and STA processing along with information on all potential biometric matches.

5. The CIMS shall forward applications without biometric duplicate matches to the TSA for STA processing.

6. The CIMS shall associate the application with the GUPID returned by the TSA. This will either be the new GUPID previously generated by CIMS for this application, or an existing GUPID if the TSA biometric match resolution indicates that this application is associated with an individual already in the CIMS database.

7. The CIMS shall notify the EP associated with an application with a TSA STA status of "Reject" that the application was rejected.

8. The CIMS shall ensure that the quality of iris images (optionally enrolled by the RT Applicant) satisfies the quality requirements specified in Section 3, Biometric Data Management and Use, by rejecting images that fail to meet the quality requirements.

9. The CIMS shall build the authentication payload, consisting of the biometric information (e.g., fingerprint templates, iris images) and the Payload ID (SPID, RTID, ADSN, and expiration date) for any applications with a TSA STA status of "Accept."

10. The CIMS shall digitally sign the authentication payload and send it to the EP.

11. Once the application has been resolved (either rejected or accepted and payload received by EP), the CIMS shall update its own database with the status of the application, update its biometric database with the Applicant's biometrics, and then delete all biographic information (including facial image and scanned identity source documents).

2.4.2 Card Issuance

The following use case outlines the steps involved in the card issuance process, including typical card issuance as well as error conditions.

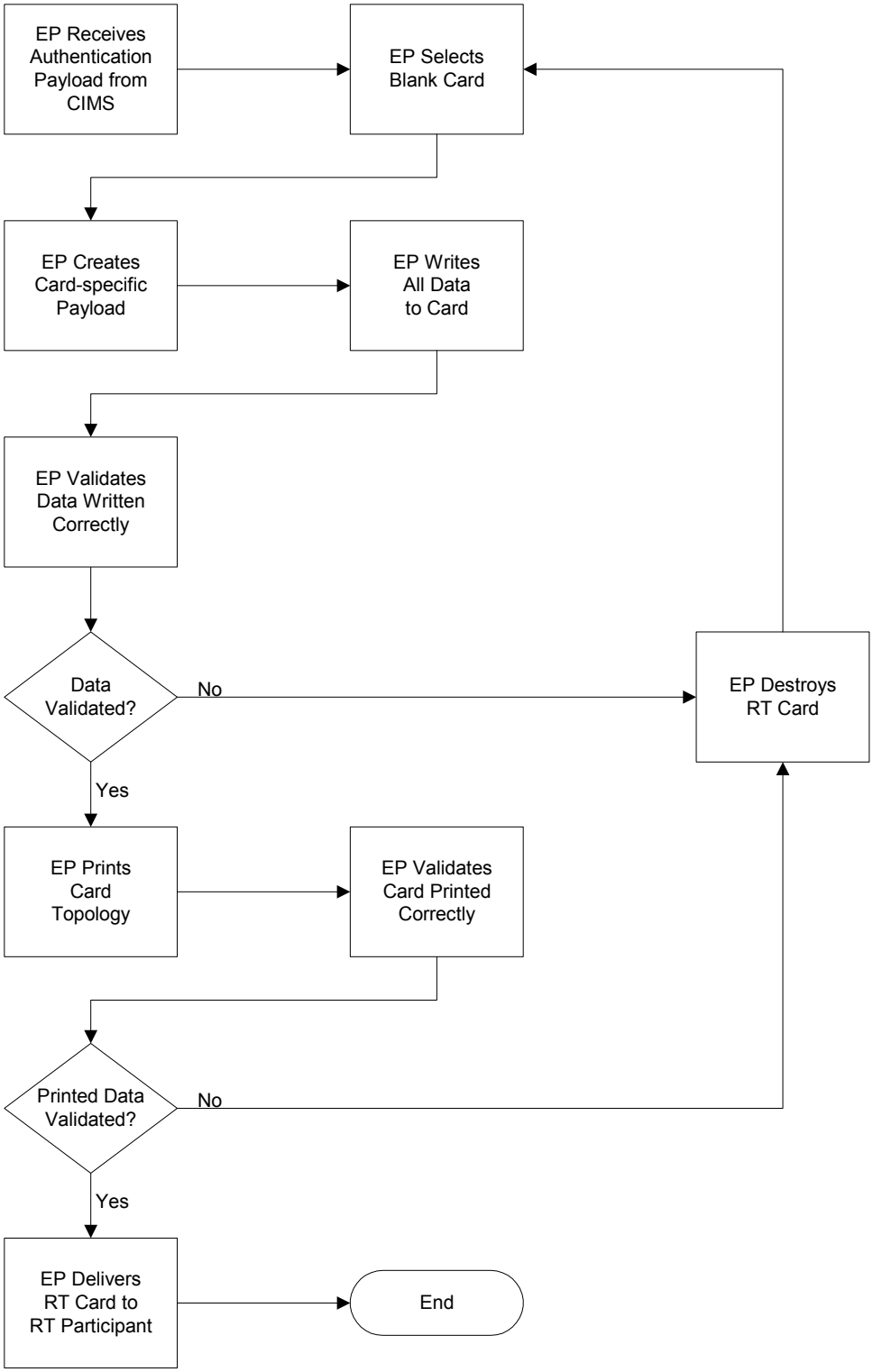


Figure 2-15. Card Issuance

Main Flow

The following process outlines the steps involved in a typical card issuance:

1. The EP receives and verifies signed authentication payload from the CIMS for an approved RT Applicant, who is now an RT Participant. The EP sends a message to the CIMS confirming receipt of the authentication payload.

2. **Select Blank Card**. The EP selects blank card stock to be used.

3. The EP creates the card-specific payload, consisting of RTUID (Payload ID and VID) and EP-specific (non-RT) data (e.g., benefit programs).

4. The EP writes data to the card, placing the CIMS authentication payload, the VID, and the EP's card-specific payload into the card.

5. The EP validates that the data in the card was written correctly.

6. If an error is detected in the data written to the card, flow passes to exception flow "Card Write Error."

7. Card topology printed, including the RT Participant's name and the RT logo.

8. The EP Enrollment Officer performs manual validation, ensuring that the information printed on the card is correct and of sufficient quality.

9. If the print on the card is of insufficient quality, flow passes to exception flow "Card Write Error."

10. The EP delivers the card to the RT Participant via a TSA approved delivery method.

Exception Flow – Card Write Error

The following exception flow describes the steps by which cards are processed if it is determined that an error occurred during card production:

1. The EP destroys the card. It is not necessary to track destroyed cards, as the raw card stock is not tracked and the same authentication payload will be used for the new card. Although it is conceivable that the card might not be destroyed, the Enrollment Provider is a trusted agent who innately possesses the ability to create multiple cards with the same payload.

2. Flow returns to main flow at "Select Blank Card". It is not necessary to ask the CIMS for a new authentication payload (with incremented ADSN) if the card was never issued and the connection between the card and payload was never established.

Card Issuance Requirements

The following are a high level set of requirements that must be satisfied by the various actors within the card issuance process:

EP Requirements

1. The EP shall not issue more than one active card to an RT Participant, other than through an optional 14 day grace period used when issuing a replacement card.

2. The EP shall acknowledge receipt of the authentication payload from the CIMS.

3. The EP shall verify signed payloads received from the CIMS.
4. The EP shall create a card-specific payload, consisting of RTUID (Payload ID and VID) and optionally, EP-specific (non-RT) data.
5. The EP shall place digital information on the card, including signed biometric payload, signed Payload ID, VID, and EP-specific benefit information.
6. The EP shall verify the information written to the card.
7. The EP shall ensure that the card topology is in a format consistent with TSA standards for RT.
8. The card shall include an RT logo on the outside, as well as the participants name.
9. The card shall include, on the outside of the card, language to be set forth in the TSA standards for RT indicating that the card is not valid US Government identification and that penalties may be levied for fraudulent or unauthorized use.
10. The EP Enrollment Officer shall verify accuracy and quality of the card topology.
11. The EP shall destroy the RT card if either the card topology or the card's payload cannot be verified.
12. The EP shall deliver the card to the RT Participant.

2.4.3 RT Participant Verification

The following use case outlines the steps involved in the verification process, including typical verification flow, the card failing to validate, the card being not authorized, and biometric authentication failure. A more detailed sequence to the authentication process performed by the verification station is given in Section 6.1.3, Card Creation and Authentication.

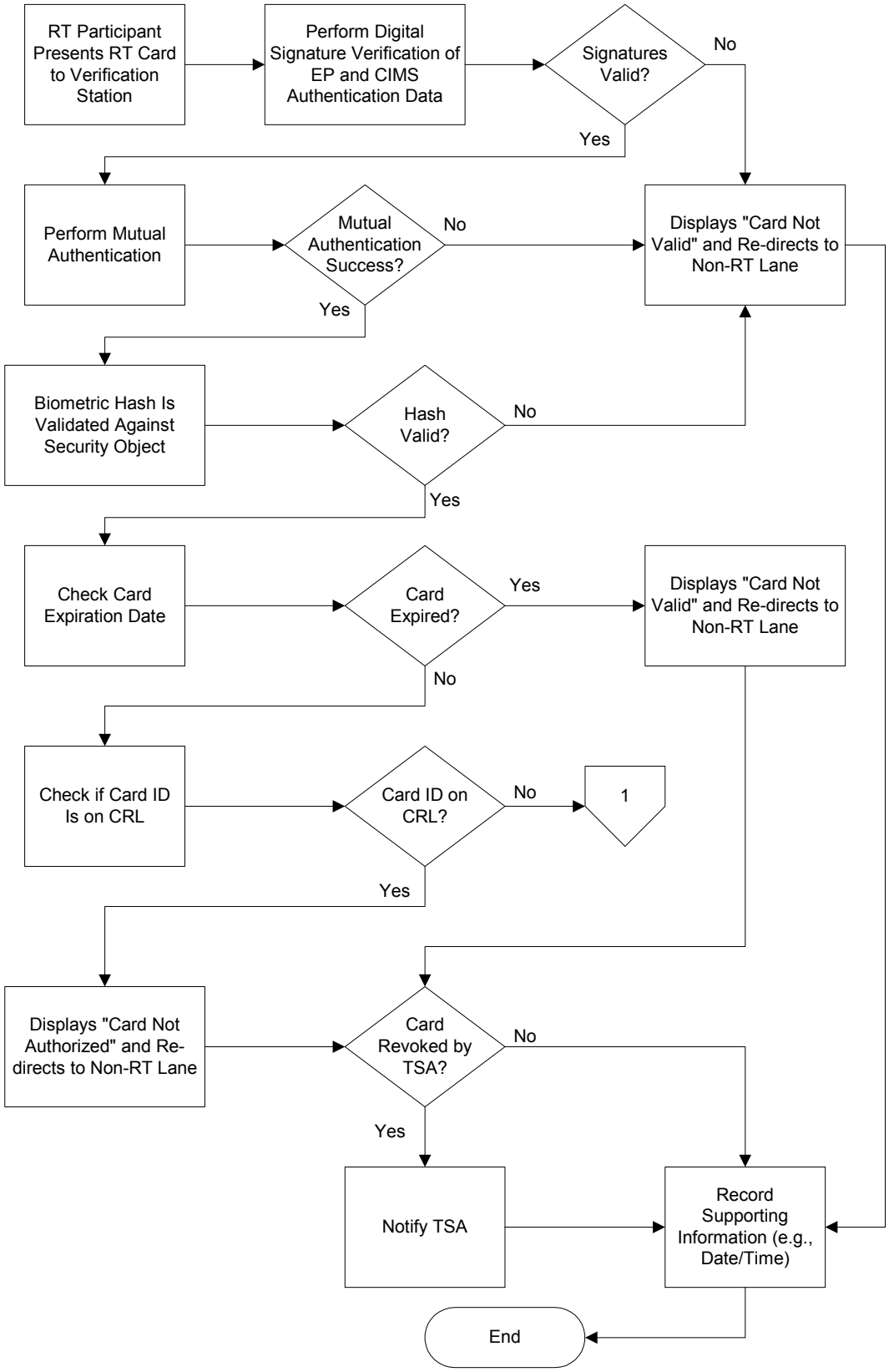


Figure 2-16. Verification (1 of 2)

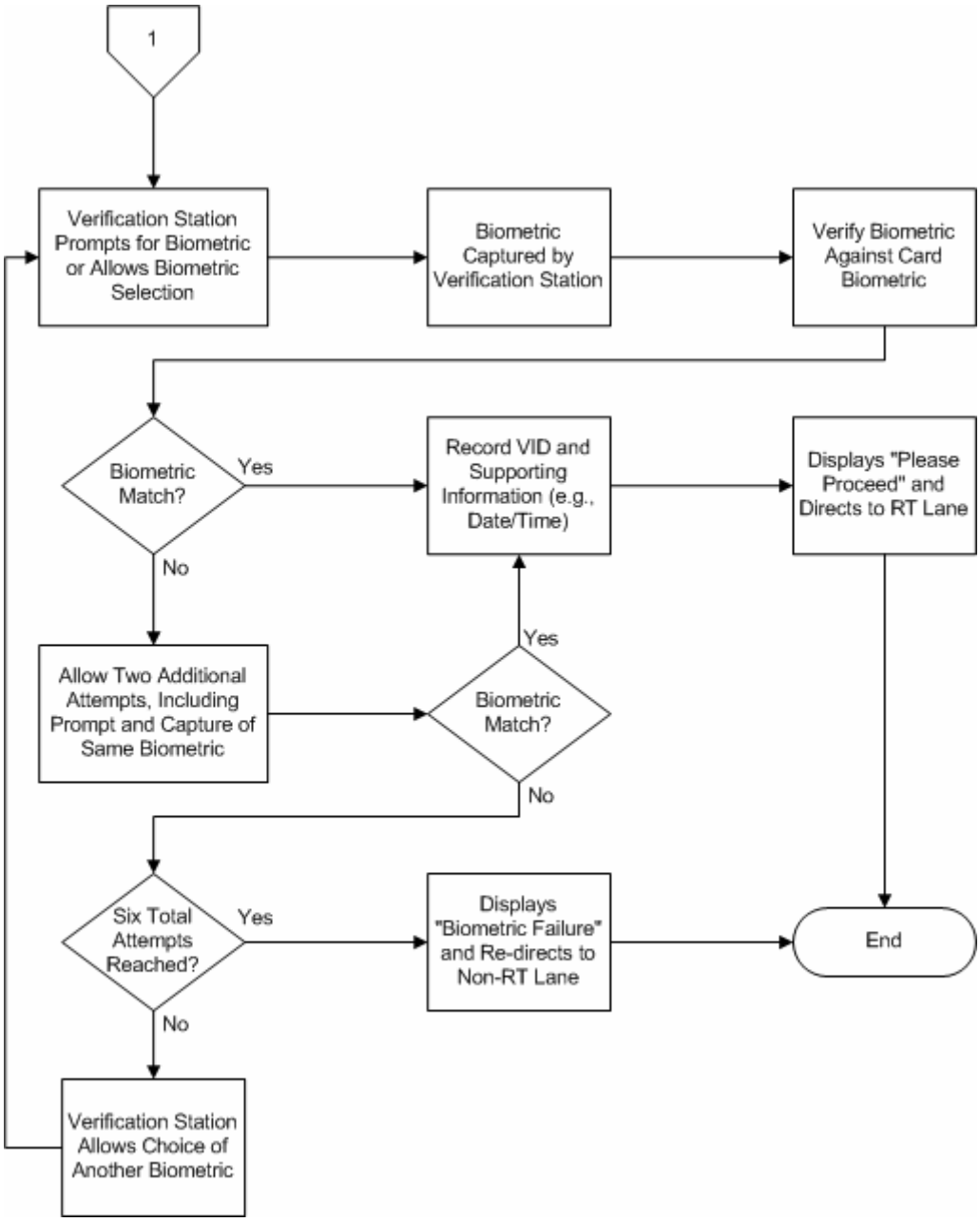


Figure 2-17. Verification (2 of 2)

Main Flow

The following process outlines the steps involved for an RT Participant to verify their identity and authorization to use RT services:

1. RT Participant presents RT card at verification station.

2. The verification station checks the security protocols of the card (i.e., digital signatures) to ensure that the card was issued by a valid EP and the authentication data was issued by the CIMS.

3. If the digital signatures on the data are not valid, the flow passes to exception flow “Card Not Valid.”

4. If the digital signatures on the data are valid, mutual authentication takes places.

5. If mutual authentication fails, the flow passes to exception flow “Card Not Valid” (although mutual authentication may fail due to a problem with the verification station).

6. If mutual authentication succeeds, the matching biometric is read from the RT Card and the hash is computed and compared to that contained within the security object.

7. If the hash is not valid, flow passes to exception flow “Card Not Valid.”

8. If the hash is valid, the verification station checks to see if the RT card is expired.

9. If the RT card is expired, flow passes to exception flow “Card Not Valid.”

10. If the RT card is not expired, the verification station compares the Card ID on the RT card to the CRL to determine if the card is on the CRL.

11. If the RT card is on the CRL, the flow passes to exception flow “Card Not Authorized.”

12. If the RT card is not on the CRL, the verification station prompts the RT Participant to present a biometric for capture as indicated by the biometric preference flag contained on the RT card. The verification station either prompts for the primary biometric preference (specified on the card), or allows the RT Participant to select the desired biometric (from a list which must have the primary biometric preference available).

13. The biometric is captured by the verification station.

14. The verification station performs a 1:1 match of the presented biometric captured to the biometric information (e.g., fingerprint template) on the card.

15. If the presented biometric does not match the biometric information on the card, the flow passes to exception flow “Biometric Failed to Authenticate.”

16. **Biometric Match**. The verification station records the VID, as well as the supporting information (e.g., verification successful, biometric used, date/time of verification, location of verification). The verification station does not retain the biometrics or the RTID from the card.

17. The verification station displays “Please Proceed.” The RT Participant removes the RT card and proceeds to the RT security lane.

Exception Flow – Card Not Valid

The following exception flow describes the process that occurs if it is determined that the card being offered by the RT Participant is expired or if the security protocols such as the digital signatures and biometric hash cannot be read or have been tampered with on the card:

1. If the card is not valid, the verification station displays a “Card Not Valid” message to the RT participant. At this time, no enforcement action is planned at the verification station.

2. The RT card is returned to the RT Participant. The RT Participant may be redirected to the non-RT airport checkpoint screening lanes.

3. If this card was invalid due to card expiration, then the VP checks to determine whether the card was revoked by the TSA, and notifies the TSA if true.

4. The verification station records the VID and any supporting information (e.g., invalid card read, date/time of attempt, location of attempt). The verification station does not retain the biometrics or the RTID from the card; however, if the card was revoked by the TSA (regardless of expiration), the RTID will be required in order to report the attempt to the TSA.

Exception Flow – Card Not Authorized

The following exception flow describes the process that occurs if it is determined that the card being offered by the RT Participant is not authorized to access RT services because of placement on the CRL:

1. If the card is not authorized, the verification station displays a “Card Not Authorized” message to the RT participant. At this time, no enforcement action is planned at the verification station.

2. The RT card is returned to the RT Participant. The RT participant may be re-directed to the non-RT airport checkpoint screening lane.

3. The VP checks to determine whether the card was revoked by the TSA, and notifies the TSA if true.

4. The verification station records the VID, as well as the supporting information (e.g., verification not authorized, date/time of attempt, location of attempt). The verification station does not retain the biometrics or the RTID from the card; however, if the card was revoked by the TSA (regardless of expiration), the RTID will be required in order to report the attempt to the TSA.

Exception Flow – Biometric Failed to Authenticate

The following exception flow describes the process that occurs if it is determined that the biometrics of the RT Participant do not match the biometrics stored on the RT card. The steps below describe a specific scenario in which the applicant gets three chances to authenticate using his primary biometric, followed by three chances to authenticate using his secondary biometric. This is shown as an example; VPs may utilize other means, as long as the RT Participant is allowed to utilize his preferred biometrics and the resulting false accept rate and false reject rate conform to the requirements specified in the Biometrics portion of this specification. RT Participants must authenticate their biometrics within a maximum of six total attempts.

1. If a 1:1 match between the presented biometric captured at the verification station and the associated biometric information (e.g., fingerprint template) on the card is not made on the first attempt, the RT Participant will be prompted to try again. The RT Participant will have a total of three attempts to sufficiently match their initial biometric preference (either the primary biometric preference or a Participant-selected biometric). If the biometric match is successful, flow returns to main flow at “Biometric Match.”

2. If a 1:1 match is not made after three attempts, the verification station will either prompt for the secondary biometric preference (specified on the card), or allow the RT Participant to select another desired biometric (from a list which must have the secondary biometric preference available). If the biometric match is successful, flow returns to main flow at "Biometric Match."

3. If a 1:1 match is not made on the first attempt at the second biometric, the RT Participant will be prompted to try again. The RT Participant will have a total of three attempts to sufficiently match the second biometric. If the biometric match is successful, flow returns to main flow at "Biometric Match."

4. If a 1:1 match cannot be made within the allowable maximum number of six total attempts, the verification station displays a "Biometric Failed to Authenticate" message to the RT Participant. At this time, no enforcement action is planned at the verification station.

5. The RT card is returned to the RT Participant. The RT Participant may be redirected to the non-RT airport checkpoint screening lanes.

6. The verification station records the VID, as well as the supporting information (e.g., biometric failed to authenticate, biometric used, how many attempts, date/time of attempt, location of attempt). The verification station does not retain the biometrics or the RTID from the card.

Verification Requirements

The following are a high level set of requirements that must be satisfied by the various actors within the verification process:

VP Requirements

1. Employees of RT Service Providers that are involved with the RT program at an airport, operate an RT component or have access to RT Applicants' personal data shall first be vetted as required by the TSA. Depending on their job location and duties, RT Service Provider employees may also need to obtain a Security Identification Display Area (SIDA) badge.

2. The verification station shall initiate the verification process when the RT Participant inserts an RT Card.

3. The verification station shall validate the card, using security protocols outlined elsewhere in this specification (e.g., digital signatures, mutual authentication, biometric hashes).

4. The verification station shall determine if the credential is authorized by determining whether the card is on the CRL.

5. The verification station shall reject an RT card that appears on the CRL and display "Card Not Authorized."

6. The verification station shall reject an RT card that is not valid or has expired and display "Card Not Valid."

7. The verification station shall deny access to the RT lane if the RT Participant is rejected (e.g., card not valid, card not authorized, biometric authentication failure). At the discretion of the TSA and the airport, RT Participants who cannot be biometrically verified due to a technical error may have direct access to a non-RT lane where feasible.

8. The verification station shall accept RT cards that are both valid and authorized, either prompting the RT Participant to provide their primary biometric preference (specified on the card) or select a biometric to be used (from a list which must have the primary biometric preference available).
9. The verification station shall capture the presented biometric and perform a 1:1 comparison with the associated biometric stored on the card.
10. Biometric authentication shall take less than two seconds per attempt, not counting RT card presentation, card data transfer, or RT Participant presentation time.
11. Additional biometric authentication attempts shall be made if the initial biometric authentication fails. Overall, the measured biometric performance of the verification station (in terms of false accept and false reject rates) shall conform to the guidelines in the Biometric portion of this specification. This may be achieved by allowing the participant three attempts with their primary biometric and three attempts with their secondary biometric, or through some other process of fusing attempts to create a final decision.
12. The verification station shall allow the RT Participant to use the secondary biometric preference as specified on the RT card if a second biometric is required.
13. The RT Participant shall be rejected, indicated by the text “Biometric Failed to Authenticate” on the verification station, if all biometric authentication attempts fail.
14. The verification station shall prompt the RT Participant to proceed through the RT lane if biometric authentication succeeds.
15. The verification station shall record, at a minimum, the VID (for billing purposes), the date/time, and the location for successful verification transactions.
16. The verification station shall not record the biometrics or the RTID of the card associated with the verification transaction. However, if the RT Participant was rejected due to a TSA revocation, more specific information (e.g., RTID) may need to be recorded.
17. The VP shall record any and all metrics required by the TSA when operations are complete, whether the RT Participant is accepted or rejected.
18. The verification station shall return the card to the RT Participant when operations are complete, whether the RT Participant is accepted or rejected (e.g., card not valid, card not authorized, biometric authentication failure).
19. The VP shall provide any and all metrics required by the TSA to the TSA in a manner and frequency to be specified by the TSA.

2.4.4 Card Re-issuance

The following use case outlines the steps involved in the card re-issuance process:

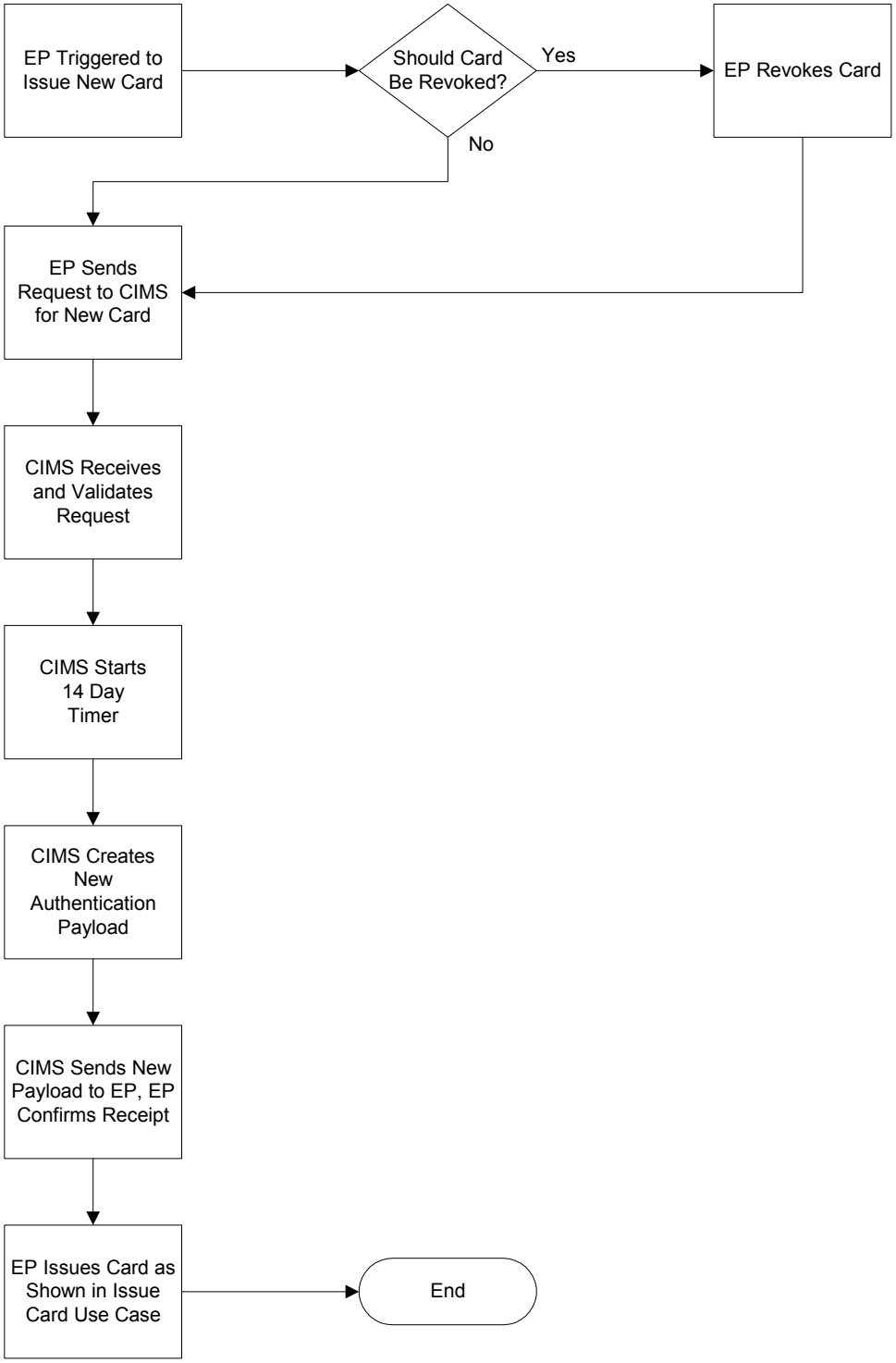


Figure 2-18. Card Re-issuance

Main Flow

The following process outlines the steps involved for an EP to re-issue a new card for an RT Participant:

1. The EP is triggered to issue a new card (e.g., card expires or RT Participant requests new card because card lost, stolen, damaged or destroyed).
2. The EP determines whether the card should be revoked immediately. The CIMS will automatically allow a grace period during which the original card is valid, to allow time for the new card to be shipped. But if the card was reported lost, stolen, destroyed, or is otherwise not usable by the RT Participant, then the EP immediately revokes the existing card (see Revocation Use Case). If the card must be replaced for any reason (i.e., intermittently failing) but is still working, the EP will not explicitly revoke the card, thereby taking advantage of the grace period to use the current card while the new card is created and delivered.
3. The EP sends a request for a new card to the CIMS.
4. The CIMS receives the request for a new card and validates the request.
5. The CIMS will start an internal 14 day timer. During this time, both the existing and re-issued cards will be active. At the end of this period, the CIMS will automatically revoke the first card.
6. The CIMS creates a new authentication payload. This will include a new Payload ID (same SPID, same RTID, incremented ADSN, and expiration date which may or may not be same).
7. The CIMS digitally signs the new authentication payload and sends this to the EP. The EP must confirm receipt of authentication payload.
8. The EP issues a new card to the RT Participant following the process described in the Card Issuance Use Case.

Card Re-issuance Requirements

The following are a high level set of requirements that must be satisfied by the various actors within the card re-issuance process:

EP Requirements

1. The EP shall revoke the RT card (as detailed in Section 2.4.5, Revocation) if the RT Participant reports that the current card is destroyed or out of their control (e.g., stolen, lost).
2. If an RT Participant requires a new card, the EP shall send a request for a new authentication payload to the CIMS, including the Payload ID of the current card.
3. If the EP receives a valid authentication payload in response from the CIMS, the EP shall create a new card for the RT Participant upon receipt of a valid authentication payload from CIMS, in accordance with the Card Issuance use case.

CIMS Requirements

1. If the CIMS receives a request for a new card, the CIMS shall start an internal 14 day timer for the first card. The first card shall be revoked after the 14 day timer has expired, unless the card has been explicitly revoked by the EP prior to that.
2. The CIMS shall build a new authentication payload that increments the Payload ID and includes the existing biometric information.

3. The CIMS shall digitally sign the payload and transmit the payload to the EP.

2.4.5 Revocation

The following use case outlines the steps involved in the revocation process. There is no process flow diagram, because there are only two or three steps for a given request.

Main Flow

The following process outlines the steps involved in revoking/suspending/reinstating an EP, an RT Participant, or a specific card. There are no sequential processes involved. Each step is a stand-alone condition based on the action desired:

Revoke

1. If the CIMS receives a request from the TSA to revoke an EP, the CIMS:
   - Enters an EP Revocation entry (SPID only) on the CRL to revoke all of the active cards (e.g., not expired, not already revoked) issued by the EP.
   - Notifies the revoked EP.
2. If the CIMS receives a request from the TSA to revoke an RT Participant's participation in the RT program, the CIMS:
   - Enters an RT Participant Revocation entry (SPID+RTID) on the CRL for each EP with which the RT Participant has an active relationship to revoke all of the active cards associated with the RT Participant (regardless of issuing EPs).
   - Notifies each of the EPs associated with those cards that are revoked.
   - Specifies that the revocation was TSA-dictated, so that future use of such revoked cards may be noted even past the expiration of the card.
3. If the CIMS receives a request from an EP to revoke an RT Participant, the CIMS:
   - Enters an RT Participant Revocation entry (SPID+RTID) on the CRL to revoke all of the active cards associated with the RT Participant that were issued by the requesting EP.
   - Notifies the TSA if the RT Participant does not have a current subscription with another EP, as the TSA can now stop the ongoing STA on the individual.
4. If the CIMS receives a request from an EP to revoke a specific RT card, the CIMS enters a Card ID entry (SPID+RTID+ADSN) on the CRL to revoke the card if the card is active and was issued by the requesting EP.

Suspend

5. If the CIMS receives a request from the TSA to suspend an EP, the CIMS
   - Enters the EP's SPID on the CRL to suspend all of the active cards that were issued by the EP.
   - Notifies the suspended EP.

6. If the CIMS receives a request from the TSA to suspend an RT Participant's participation in the RT program, the CIMS:

    - Enters the RT Participant's SPID+RTID on the CRL for each EP with which the RT Participant has an active relationship to suspend all active cards associated with the RT Participant (regardless of issuing EPs).

    - Notifies each of the EPs associated with those cards that are suspended.

7. If the CIMS receives a request from an EP to suspend an RT Participant, the CIMS enters the RT Participant's SPID+RTID on the CRL to suspend all of the active cards issued by the requesting EP that are associated with the RT Participant.

8. If the CIMS receives a request from an EP to suspend a specific RT card, the CIMS enters the Card ID on the CRL to suspend that specific card if the card is active and was issued by the requesting EP.

Reinstate/Removal from CRL

9. If the CIMS receives a request from the TSA to reinstate a suspended EP, the CIMS:

    - Reinstates all of the cards that would be active without the TSA suspension (e.g., not expired, revoked, or suspended by the EP) that were issued by the EP by removing the EP's SPID from the CRL.

    - Notifies the EP.

10. If the CIMS receives a request from the TSA to reinstate a suspended RT Participant, the CIMS:

    - Reinstates all of the cards that would be active without the TSA suspension (e.g., not expired, revoked, or suspended by the EP) that were associated with the RT Participant (regardless of issuing EP) by removing the RT Participants SPID + RTID from the CRL for each EP (unless the EP also requested suspension/revocation).

    - Notifies each of the EPs associated with those cards that are reinstated.

11. If the CIMS receives a request from an EP to reinstate a suspended RT Participant, the CIMS reinstates all of the cards that would be active without the EP suspension (e.g., not expired, revoked, or suspended by the TSA) that were associated with the RT Participant and issued by the requesting EP by removing the SPID + RTID from the CRL (unless the TSA also requested suspension/revocation).

12. If the CIMS receives a request from an EP to reinstate a suspended RT card, the CIMS reinstates the card if the card would be active without the EP suspension (e.g., not revoked) and the card was issued by the requesting EP, by removing that specific Card ID from the CRL.

Revocation Requirements

The following are a high level set of requirements that must be satisfied by CIMS within the revocation process. Revocation requirements for EPs and VPs are detailed in Enrollment Requirements and Verification Requirements, respectively.

CIMS Requirements

Revoke

1. If the CIMS receives a request from the TSA to revoke an EP, the CIMS shall revoke (using the CRL) all of the active cards (i.e., not expired or already revoked) issued by the EP and notify the EP.

2. If the CIMS receives a request from the TSA to revoke an RT Participant's participation in the RT program, the CIMS shall revoke (using the CRL) all of the active cards (i.e., not expired or already revoked) associated with the RT Participant (regardless of issuing EP).

3. If the CIMS receives a request from the TSA to revoke an RT Participant's participation in the RT program, the CIMS shall notify each of the EPs associated with those cards that are revoked.

4. If the CIMS receives a request from the TSA to revoke an RT Participant's participation in the RT program, the CIMS shall record that the revocation was TSA-dictated, so that future use of such revoked cards may be noted even past the expiration of the card.

5. If the CIMS receives a request from an EP to revoke an RT Participant, the CIMS shall revoke (using the CRL) all of the active cards (i.e., not expired or already revoked) associated with the RT Participant that were issued by the requesting EP.

6. If the CIMS receives a request from an EP to revoke an RT Participant, the CIMS shall notify the TSA if the RT Participant does not have a current subscription with another EP, as the TSA can now stop the ongoing STA on the individual.

7. If the CIMS receives a request from an EP to revoke a specific RT card, the CIMS shall revoke (using the CRL) that specific card if the card is active (i.e., not expired or already revoked) and was issued by the requesting EP.

Suspend

8. If the CIMS receives a request from the TSA to suspend an EP, the CIMS shall suspend (using the CRL) all of the active cards (i.e., not expired or revoked) that were issued by the EP and notify the EP.

9. If the CIMS receives a request from the TSA to suspend an RT Participant's participation in the RT program, the CIMS shall suspend (using the CRL) all of the active cards (i.e., not expired or revoked) associated with the RT Participant (regardless of issuing EP).

10. If the CIMS receives a request from the TSA to suspend an RT Participant's participation in the RT program, the CIMS shall notify each of the EPs associated with those cards that are suspended.

11. If the CIMS receives a request from an EP to suspend an RT Participant, the CIMS shall suspend (using the CRL) all of the active cards (i.e., not expired or revoked) that are associated with the RT Participant and were issued by the requesting EP.

12. If the CIMS receives a request from an EP to suspend a specific RT card, the CIMS shall suspend (using the CRL) that specific card if the card is active (i.e., not expired or revoked) and was issued by the requesting EP.

Reinstate

13. If the CIMS receives a request from the TSA to reinstate a suspended EP, the CIMS shall reinstate (using the CRL) all of the cards that would be active without the TSA suspension (e.g., not expired, revoked, or suspended by the EP) that were issued by the EP and notify the EP.

14. If the CIMS receives a request from the TSA to reinstate a suspended RT Participant, the CIMS shall reinstate (using the CRL) all of the cards that would be active without the TSA suspension (e.g., not expired, revoked, or suspended by the EP) that were associated with the RT Participant (regardless of issuing EP).

15. If the CIMS receives a request from the TSA to reinstate a suspended RT Participant, the CIMS shall notify each of the EPs associated with those cards that are reinstated.

16. If the CIMS receives a request from an EP to reinstate a suspended RT Participant, the CIMS shall reinstate (using the CRL) all of the cards that would be active without the EP suspension (e.g., not expired, revoked, or suspended by the TSA) that were associated with the RT Participant and issued by the requesting EP.

17. If the CIMS receives a request from an EP to reinstate a suspended RT card, the CIMS shall reinstate (using the CRL) the card if the card would be active without the EP suspension (e.g., not expired, revoked, or suspended by the TSA) and the card was issued by the requesting EP.

2.5 RT Program Requirements

Beyond the schematics and diagrams outlined in this section, there are several qualitative and policy requirements necessary to ensure interoperability between Service Providers. The following high-level requirements are based on the TSA's May 25, 2006 RT Model, the RTIC's RFI Submissions, and war-room discussions with the TSA. The TSA will be responsible for outlining all of the RT program requirements. This section is for requirements that are not found elsewhere. For instance, high-level security requirements can be found in Section 6, System Security.

Some of these are listed here for completeness and to provide a broader overview.

2.5.1 Privacy Requirements

The following requirements pertain to policy procedures that must be in place to ensure the privacy of RT Applicants and RT Participants:

- The EP must establish a written privacy policy to govern the data collected in connection with the RT program and must provide this policy, in writing, to each eligible RT Applicant.

- The EP must provide each eligible RT Applicant with a copy of the Federal Privacy Act at the time of enrollment.

- The EP must not disclose biographic and/or biometric data required for the purposes of the RT program and collected by the EP from RT Applicants and RT Participants other than for RT purposes. Disclosure of data will be governed by the government's RT Privacy Impact Statement (PIA).

- The EP must not store, use, sell, or disseminate any biographical and/or biometric data collected for the purpose of the RT program and collected by the EP from the RT program Applicants or Participants for any commercial purposes without the approval of the RT Applicant or RT

Participant, other than for RT purposes. The request to RT Applicants for permission for storage, use, sale, and/or dissemination of their data must be comprehensible and concise. The EP must delete the biometric information, unless otherwise explicitly permitted.

2.5.2 General RT Principles

The following represent general RT principles:

- Sponsoring Entities must:
    - Be an airport or air carrier.
    - Select and qualify all participating Service Providers.
    - Contract directly with EP/VP vendors, rather than through the TSA.
    - Determine whether to contract with one or two Service Providers to provide enrollment and verification services. An RT Service Provider may provide either enrollment or verification services or both services.
- The interoperability of any SP must be verified before the TSA gives final approval for participation in the program.
- Both Enrollment Providers and Verification Providers must:
    - Allow TSA or its contractors to conduct audits or inspections.
    - Be interoperable with other Service Providers.
    - Belong to the CIMS network.
    - Be authorized via the TSA's Verification and Validation process. SPs are subject to V&V oversight by the Sponsoring Entity and the TSA. This includes ensuring that all personnel (EP, card production, VP, etc.) who handle RT Applicants' and Participants' personal information are properly trained and vetted to perform necessary enrollment procedures and use required technology.
    - Ensure that information in the enrollment and verification stations is protected against compromise through encryption technologies and physical security configuration in accordance with TSA standards.
    - Be sponsored by a Sponsoring Entity and must comply and remain in compliance with TSA-issued RT standards.
    - Ensure that interoperability testing through the CIMS, focusing on the technology and accompanying software, occurs prior to operation.
- Enrollment Providers must:
    - Submit a TSA fee per RT Applicant enrollment (and per RT Participant renewal) through the CIMS. The non-refundable fee will be a flat amount paid initially at enrollment and on an annual per RT Participant renewal basis.
    - Maintain a website that shall include privacy policies, a list of acceptable enrollment documents, and additional benefits, as well as instructions/functions to pay user fees.

  - Ensure that any information collected for non-RT purposes must be through an “opt-in” process and must be clearly identified as non-RT related data.
  - Refrain from selling or disseminating any biographic and/or biometric data collected by EPs from RT Applicants for any commercial purposes without the explicit approval of the RT Applicant and the Sponsoring Entity.
  - Issue and deliver RT cards to RT Participants through an approved TSA mechanism.

- Verification Providers must:
  - Ensure that the TSA has first evaluated and approved any new security technology that may be deployed at RT lanes.
  - Refrain from storing RT Participants’ personal data except as specified. Specifically, the RTID shall not be retained unless specified by the TSA for TSA revocation purposes only.
  - When an RT Participant is successfully verified at a verification station, the station must indicate success. The VP must ensure that only RT Participants who have successfully verified at a verification station are allowed to proceed through the RT security lane. For example, direct and dedicated access from the verification station to the RT security lane may be provided, or the RT Participants boarding pass may be marked in such a way as to maintain the level of security provided by the rest of the RT system.
  - Provide the CIMS with a weekly report of attempts to use an RT card that was revoked by the TSA.
- RT Participants must:
  - Be US citizens, nationals, or lawful permanent residents (LPR).
  - Be the age of 12 or greater. Minors under the age of 12 are not eligible to join RT but may access the RT line with a parent or legal guardian that is an RT participant. Minors over the age of 12 are eligible to join on the same basis and through the same process as adults with the additional requirement that a parent or legal guardian must be an approved RT.
  - Be able to receive and maintain an approved STA determination.
  - Agree to abide by the terms provided to them by the EP during the enrollment process and must remain current in the payment of user fees.
- At no time will the RT card be considered a valid US Government identification credential.
- The CIMS must:
  - Comply with all applicable privacy requirements as defined by the TSA.
  - Refrain from selling or disseminating any biographic and/or biometric data collected by EPs from RT Applicants for any commercial purposes.
  - For each RT Participant, the CIMS will store, among other things, the RTID, biometric information, enrollment submission date, an approved or not approved STA finding, and any other information as directed by TSA.

  - Monitor the enrollment dates of all RT Participants and deactivate RT membership in the absence of renewal.
  - Act as an information broker between the SPs and the TSA, ensuring that the databases maintained by the SPs, CIMS, and the TSA remain synchronized. This will be done on a monthly basis.

- The TSA must:
  - Communicate the results of the STAs to the CIMS after an STA determination is reached. TSA will not transmit details about the STA or the reasons behind the determination.
  - Communicate the results of duplicate adjudication.
- All SP, TSA, CIMS, Sponsoring Entities and other US Government or private sector entities that will handle RT data must provide a fully integrated, layered, security structure as approved by the TSA V&V process which is built on industry standards for identity management systems.
- All personal data must be encrypted at the initial collection point.
- All data transfers require authentication of participants at both ends and all identity information (including RTID and RTUID container) used in the verification process shall be verified using digital signatures to ensure data integrity and chain-of-trust from CIMS and the EP.

The CIMS and US Government systems must meet all FISMA requirements. All SPs must be in compliance with TSA standards as defined in the V&V document that will be based on FISMA.

2.6 Participant Group Processing Rules

There are different business rules for each of the participant categories (subpopulations) identified in Section 2.2.2 when they are processed by the Central Identity Management System (CIMS).

For RT participants (RTPART), CIMS will process the enrollment as defined in section 2.4 above. (That is, CIMS sends the enrollment record to TSA. TSA will perform a Security Threat Assessment (STA) against them. TSA will return a Green or Red indication. If Green, a payload will be generated and sent to the SP to issue an RT card. The payload message will have the RTCN used on the enrolment message so that the response message will not be confused with a response message from another subpopulation.

For SP officers or employees (SPOFFICER or SPEMPLOYEE), CIMS will process the enrollment record and send it to TSA. TSA will perform a STA as well as a Criminal History Records Check (CHRC) on these individuals. A response message will be sent to the SP, but it will not include a payload. The response message will have the RTCN used on the enrollment message so that the response message will not be confused with a response message from another subpopulation.

For those in the pilot group (RTPILT), there will not be an STA performed in the initial year of participation since these individuals will have had an STA done in the pilot program. A payload will be generated to the SP to issue an RT card. The payload message will have the RTCN used on the enrollment message so that the response message will not be confused with a response message from another subpopulation.

> NOTE: On the initial anniversary date of the RTPILT enrollment submission, the individual will be renewed in the RT program as outlined in the specification. During this renewal, their subpopulation will change within CIMS from RTPILT to RTPART.

The following sections define the business rules for handling changes in participant category (i.e., when an employee or officer wants to obtain an RT card for use).

Case 1 – A Participant becomes an Employee or Officer

If an existing RTPART or RTPILT becomes an employee or officer of a SP, CIMS will already have their initial RTID and will have generated a payload for them.

The SP will need to transmit the individual's information to CIMS with a new enrollment submission with the participant group identifier set as SPEMPLOYEE or SPOFFICER. This enrollment message will contain the same RTID as the original enrollment submission. The message will be processed and sent to TSA for a CHRC and an STA. TSA will receive a new GUPID for this individual and will also receive the GUPID for the original enrollment request. When a positive result is returned to CIMS, an acknowledgement message will be sent to the SP, but no payload will be sent. A single GUPID should thus be assigned; assuming TSA determines the second enrollment request is for the same individual. The response message will have the RTCN used on the SPEMPLOYEE or SPOFFICER enrollment message so that the response message will not be confused with a response message from another subpopulation.

Case 2 - Employee or Officer wants an RT Card

If an individual enrolls into CIMS with a participant group identifier of SPEMPLOYEE or SPOFFICER, they will be charged the program fees and sent to TSA for a CHRC and an STA. When a positive result is returned to CIMS, an acknowledgement message will be sent to the SP, but no payload will be sent.

If the individual wants to have an RT card, the SP will need to transmit to CIMS a new enrollment submission with the subpopulation identifier set as RTPART. This enrollment message will contain the same RTID as the original enrollment submission. The message will be sent to TSA for an STA only check. TSA will receive a new GUPID for this individual and will also receive the GUPID for the original employee enrollment request, based on the biometric de-duplication check done at CIMS. When a positive result is returned to CIMS, an acknowledgement message with a payload will be generated and sent to the SP. At this time a card can be issued. A single GUPID should thus be assigned; assuming TSA determines the second enrollment request is for the same individual. The payload message will have the RTCN used on the RTPART enrolment message so that the response message will not be confused with a response message from another subpopulation

Case 3 - Employee or Officer terminates employment with a SP and wants to keep the RT Card

If an individual is in multiple participant groups (SPEMPLOYEE or SPOFFICER and RTPART or RTPILT) and is being removed from the SPEMPLOYEE or SPOFFICER population, the SP will need to send a revocation message with the enumerated action type of SP_EMPLOYEE_REMOVE or SP_OFFICER_REMOVE to CIMS. CIMS will mark a flag in the database indicating this individual is not within the specified subpopulation (SPEMPLOYEE or SPOFFICER).

CIMS will send a Delete message to TSA for the GUPID/subpopulation (SPEMPLOYEE or SPOFFICER) informing TSA to delete this individual from the specified group. The GUPID will remain valid in the RTPART group, but not in the SPEMPLOYEE or SPOFFICER group.

Case 4 – Employee or Officer stays with SP but ends program participation (turns in RT Card)

If an individual is in multiple participant groups (RTPART or RTPILT and SPEMPLOYEE or SPOFFICER) and is being removed from the RTPART population, the SP will need to send a revocation message to CIMS. CIMS will mark a flag in the database indicating not to renew this individual within the specified subpopulation (RTPART) for the coming year and the card will be placed on the Card Revocation List (CRL).

CIMS will send a Delete message to TSA for the GUPID/subpopulation (RTPART) informing TSA to delete this individual from the specified group. The GUPID will remain valid in the SPEMPLOYEE or SPOFFICER group, but not in the RTPART group.

3 Biometric Data Management and Use

Biometrics are a key component of RT, serving in a number of capacities. This section identifies the biometric technologies, uses, formats, and standards as they apply to the RT program.

3.1 Biometric Technology Selections

The following biometrics have been selected for use with RT:

- Fingerprint - Fingerprint images shall be collected from each RT Applicant.
- Iris - At the discretion of the RT Applicant, iris images may be collected.
- Facial - A facial photograph shall be collected from each RT Applicant.

3.2 Biometric Uses within RT

3.2.1 Enrollment

Enrollment includes the process of collecting biometric samples from the RT Applicant and the subsequent preparation of the biometric data for use in the RT application process (i.e., the RT card issuance decision is predicated on steps that utilize this data).

The enrollment station will be used to collect personal data, background information, and biometric information, and to validate government-issued credentials. Some of this data may be collected during a pre-enrollment step and then confirmed during enrollment. All required biometrics shall be captured during a single enrollment session. It is important that very high quality biometric images are captured, as this is a key factor in subsequent biometric matching performance. Biometric image quality checks shall be performed at the time of capture to allow for recapture, if necessary, prior to transmitting the data to the CIMS and while the RT Applicant is present and available.

The configuration of the enrollment station is the purview of the Enrollment Provider, but is expected to include the following devices/capabilities:

- Biometric capture devices, to include:
    - Ten-print fingerprint live scan device
    - Iris camera
    - Digital camera
- Document scanner
- Document authentication capability

3.2.1.1 Fingerprint Enrollment

The enrollment process includes the collection of fingerprint biometrics. Enrollment Providers shall attempt to capture 10 flat fingerprint images from each RT Applicant. Three fingerprint slap impressions shall be captured (i.e., one image containing the left simultaneous four fingers, one image containing the right simultaneous four fingers, and one image containing two thumbs). Rolled fingerprints will not be captured. In cases where physical disability prevents an RT Applicant from providing all 10 flat fingerprint images, the Enrollment Provider shall indicate the reason that a fingerprint image could not be captured (e.g., bandaged or amputated finger). At a minimum, an RT Applicant must provide four fingerprint images of sufficient quality in order to participate in the program.

Note: A waiver may be granted for certain individuals who are unable to provide four fingerprints of sufficient quality (as defined below). This may occur, for example, in elderly applicants.

Federal Bureau of Investigation (FBI) certified electronic capture devices shall be utilized to capture fingerprint images. These devices have been certified by the FBI to meet the Integrated Automated Fingerprint Identification System (IAFIS) Image Quality Specifications (IQS) as documented in the Electronic Fingerprint Transmission Specification (EFTS), Appendix F.

Fingerprint image quality assessment is a critical element of the RT system since image quality has a direct effect on subsequent fingerprint matching performance. Quality feedback is important during enrollment to allow for recapture. Fingerprint image quality shall be assessed using the NIST Fingerprint Image Quality (NFIQ) algorithm (NISTIR 7151). The goal is to achieve quality scores of three or better. In the situation where the quality score is worse than three, at least three attempts to recapture images shall be made. If there are multiple attempts to capture fingerprint images, then the best quality images shall be utilized for enrollment. At a minimum, the Enrollment Provider shall capture four fingerprint images that pass the quality check, that is, four images with a NFIQ score of 1, 2, or 3. Failure to achieve this minimum quality score will prevent the RT Applicant from participating in the RT program. As a necessary step in assessing fingerprint image quality, individual fingerprint images must be segmented from the fingerprint slap impressions. Enrollment Providers shall verify that the segmentation algorithm accurately segmented the fingerprint images.

At the discretion of the enrollment officer, after three best effort attempts are made, a waiver may be granted to certain individuals for whom four acceptable quality fingerprint images cannot be obtained. However, in these cases, at least two fingerprints of sufficient quality are required in order to enable generation of two matchable fingerprint templates for inclusion in the card payload. When such a waiver has been granted, it will be indicated in the enrollment message so that the CIMS will not reject it, but process it using the “2 good finger” rule.

Fingerprint enrollment data shall be formatted as an XML representation of the EFTS Type-14 record, as defined in Section 4, System Messaging. This data will be transmitted to the CIMS for further processing (see Sections 3.2.2, CIMS Duplicate Checks, and Section 3.2.3, Biometric Storage on the RT Card).

3.2.1.2 Iris Enrollment

The enrollment process optionally includes the collection of iris biometrics. If an RT Applicant agrees to provide iris data, Enrollment Providers shall attempt to capture iris images from both left and right eyes. Iris capture shall be performed in accordance with manufacturer recommendations, if available. In cases where enrollment efforts, for any reason, are unsuccessful at capturing both left and right iris images, the Enrollment Provider may capture images from one eye.

Quality assessment shall be performed on captured iris images. Iris images selected for enrollment shall conform to quality recommendations of Annex A of International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 19794-6:2005 with a quality score of at least 61. In addition, the EP shall perform local image quality checks prior to submission to CIMS that include, but not limited to:

1. Iris Diameter – The iris diameter shall be greater than or equal to 170 pixels.
2. Focus – Iris images should have a focus quality adequate to preserve spatial resolution.
3. Visibility – Iris images shall contain 70% or greater unobstructed visibility of the iris.

The EP shall validate the enrollment iris images against a second set of iris images collected at the time of enrollment:

1. The enrollment iris images shall be used to locally generate a set of polar images, compliant with Section 3.3, Biometric Formats and Standards.
2. The EP shall collect a second set of iris images from the RT Applicant. It is strongly recommended that the EP cause the iris camera to re-engage the RT Applicant by requiring the RT Applicant to step away from the iris camera between the capture of the enrollment iris images and the capture of the validation iris images.
3. The EP shall match the enrollment polar images against the validation iris images (using templates derived from rectilinear images) using any matching algorithm they choose. Matching will be done at a threshold (FMR, FNMR) complaint with Section 3.4, Verification.
4. The EP shall include the iris enrollment rectilinear images with the enrollment package only if this match is successful.

Iris enrollment data shall be formatted as rectilinear images that conform to ISO/IEC 19794-6:2005, as defined in Section 3.3, Biometric Formats and Standards.

Enrollment Providers should consult Annex A of ISO/IEC 19794-6:2005 on recommended guidance when selecting an iris camera device.

This data will be transmitted to the CIMS for further processing (see Section 3.2.2, CIMS Duplicate Checks, and Section 3.2.3, Biometric Storage on the RT Card). In addition to this processing, the CIMS shall perform a second quality assessment on the iris images in regards to the reported quality score and the iris diameter. The CIMS will also generate polar images from the rectilinear images and perform a match between the polar images and rectilinear images using its own matching algorithm with a threshold compliant with Section 3.4, Verification. If the CIMS is unable to generate polar images, iris codes (templates), or perform a successful match between the two, then the affected iris enrollment will be deemed invalid and not included in the returned authentication payload.

3.2.1.3 Face Enrollment

The enrollment process includes the collection of a digital photograph of the RT Applicant's face. Enrollment Providers shall capture a basic facial color photograph from each RT Applicant. Enrollment Providers should consult InterNational Committee for Information Technology Standards (INCITS) 385-2004, Annex A, Best Practices for Frontal Images, for guidance (as applicable) on facial image capture conditions. Facial image quality checks should be performed at the time of capture, so that recapture can be performed as necessary.

Automated facial recognition is not planned at this time.Facial image enrollment data shall be formatted as an INCITS 385-2004 record, as defined in Section 3.3, Biometric Formats and Standards. This data will be transmitted to the CIMS.

3.2.2 CIMS Duplicate Checks

To maintain the integrity of the RT system, it is important that RT cards are not issued to the same person under different identities (names). The only way to ensure this is to perform a 1:N biometric check against a central database at the CIMS, because the individual may be able to obtain identity documents under different names, but cannot change their intrinsic biometrics.

Both fingerprint and iris technologies are able to support 1:N searches of very large databases with acceptable accuracy. To fulfill the purpose of the checks, they must be done against a single (logical) database of biometric records. Per the TSA RT Model of May 2006, however, iris enrollment is optional for the RT Applicant, and consequently iris technology cannot be used at this time as the primary basis for a duplicate check. Therefore, the CIMS shall provide a 1:N matching capability for fingerprint data. Iris data may be used as a secondary means of duplicate identification in the event such information is available.

Enhanced accuracy may be achieved by performing 1:N matches of multiple features, such as multiple fingers. In this case suitable decision rules must be formulated.

Since 1:N biometric matching results in either zero matches (no hit, normal result) or a candidate list (one or more hits, occurring less often), a capability to confirm the candidate hits is required. Candidate hits can be true or false matches, and therefore the CIMS shall provide a method to determine the true matches from the false matches in the candidate match list. Use of multiple biometrics can greatly reduce the number of false matches, such as the use of iris data as mentioned above.

3.2.3 Biometric Storage on the RT Card

To support biometric verification at the verification station, the RT Participant's biometric authentication data shall be securely stored (digitally) on the RT card. The RT card shall contain the following biometric authentication data:

- Four distinct fingerprint templates (left and right index and middle fingers preferred, but any can be used).
- Two iris images in polar format (if provided).

In order to maximize interoperability and ensure the chain of trust, the CIMS shall be responsible for generating the fingerprint templates and the iris polar images for storage on the RT card. This data will be transmitted to the Enrollment Provider for use in RT card production. Formats for biometric records stored on the RT card are identified in Section 3.3, Biometric Formats and Standards. Biometrics stored on the RT card shall be packaged in Common Biometric Exchange Formats Framework (CBEFF) records, as defined in Section 3.3.3.1, CBEFF. No digital signature is required on the CBEFF record itself since security is included on the container. See Section 5, The RT Card, and Section 6, System Security, for more information on how the authentication data is secured.

For fingerprint templates, the Enrollment Provider may indicate which fingers from the fingerprint enrollment data should be included on the RT card. If these preferences are provided, and meet minimum NFIQ quality requirements, the CIMS shall attempt to generate fingerprint templates for the preferred fingers. If no preferences are provided, the CIMS shall attempt to generate fingerprint templates for the left index, right index, left middle, and right middle fingers. If the CIMS cannot generate a fingerprint template (e.g., due to poor fingerprint quality or technical error), then the CIMS shall select an alternate finger. The CIMS shall notify the Enrollment Provider which fingerprint templates were generated. If the full four fingerprint templates could not be generated, then a minimum of two will be generated for storage on the RT card. If at least two fingerprint templates could not be generated, then the enrollment application will be rejected and new biometric data will need to be captured from the RT Applicant.

The facial image data captured by the Enrollment Provider shall also be stored in the RT card. Facial image data shall not be used as biometric authentication data to verify the RT Participant's identity. See Section 5, The RT Card, for more information about storing facial image data in the RT card.

Maximum storage capacity requirements (exclusive of any associated ancillary or security data, e.g., digital signatures) are provided in Table 3-1.

Biometric	Format on RT Card	CBEFF Record Size	Total RT Card Storage Size
Fingerprint	1 to 2 CBEFF records, the first record containing 2 templates. The 2nd CBEFF record if used will contain 1 to 2 templates.	2000 bytes	4000 bytes
Iris	0 to 2 CBEFF records, each containing 1 iris image in polar format	4000 bytes	8000 bytes
Face	1 CBEFF record containing a basic facial image	17000 bytes	17000 bytes

Table 3-1. RT Card Biometric Authentication Data Maximum Storage Capacity

3.2.4 Verification

At the verification station, the identity of the RT Participant must be verified to ensure that he/she is the person to whom the RT card was issued. (Other checks are also performed to ensure that the card is still valid and privileges have not been revoked, etc., but these do not involve biometrics.)

Upon authentication and verification of a valid RT card, the Verification Provider shall match presented biometrics from the RT Participant against the enrolled biometrics stored on the RT card. This involves the following steps:

1. The RT Participant's preferred biometric option and selected biometric data are read off of the RT card.
2. The RT Participant is prompted to interact with the biometric capture device on the verification station.
3. The RT Participant presents their biometric to the sensor, and the data is captured.
4. The presented biometric data is processed for matching.
5. 1:1 matching is performed on the verification station between the enrolled biometric data obtained from the RT card and the processed presented sample obtained from the RT Participant.

If the match to the preferred biometric is successful, then the RT Participant is permitted to proceed forward in the security checkpoint process. If the match is not successful, the Verification Provider may recapture biometric data from the RT Participant and try the match again, up to three verification attempts. If a match to the preferred biometric is not made, the Verification Provider shall attempt to match to a secondary biometric stored on the RT card. The Verification Provider may make up to three verification attempts using the secondary biometric. If the match is still unsuccessful, the RT Participant will be redirected to a non-RT airport checkpoint screening lane. For this biometric verification process, the false reject rate shall not exceed 1% (1 in 100) at a fixed 1% false accept rate operating point. Verification Providers are not precluded from using more stringent false accept rate criteria. The TSA V&V procedures shall enforce these performance criteria.

Note that a Verification Provider may choose to use more than one biometric in either a layered/cascaded fashion or with true multi-biometric fusion, as long as the above false reject rate and false accept rate requirements are still met.

3.2.5 Archive and Audit

3.2.5.1 Biometric Data Archive

Archived data is needed in order to support hit confirmation, card re-issuance, and reloading of 1:N search/match engines. The CIMS shall store (archive) the following enrolled biometric data for each RT Applicant:

- Fingerprint images
- Iris images in rectilinear format (if provided).

The CIMS shall associate the stored biometric data to the SPID and RTID. The CIMS shall not store any other personal biographic information or the facial photograph in order to protect the privacy of the RT Applicant. Access control mechanisms shall be placed on the CIMS to ensure that only authorized personnel and applications can access this information.

3.2.5.2 Biometric Auditing

The CIMS, Enrollment Provider, and Verification Provider components are responsible for recording audit events, as applicable to their stated purpose. The RT system components, as applicable, shall record the following biometric-related events in an audit log:

- Biometric enrollment
- Transmission of biometric data internally (e.g., to card production) or to external systems/components (e.g., to the TSA for a security threat assessment)
- Biometric verification (e.g., verification ID)
- Biometric data storage or update (e.g., to the CIMS database/archive).

Audit records shall not contain the biometric data itself. Audit records shall not contain personal identifying information. For example, logging of a verification event should record the verification ID, but not cardholder information, such as the RTID.

Audit records shall be protected from unauthorized access and modification. Access controls and digital signing methods should be employed. Refer to Section 6, System Security, for further information.

3.3 Biometric Formats and Standards

This section identifies the biometric standards to be utilized on the RT program to facilitate interoperability and performance. Table 3-2 provides a summary of the biometric data formats.

Biometric	Enrollment Data	RT Card Data
Fingerprint	EFTS 7.1 Type-14 ▪ 3 Type-14 records, represented as XML	INCITS 378-2004 ▪ 1 to 2 CBEFF records, each containing 1 INCITS 378 record – The first INCITS 378-2004 record contains 2 fingerprint templates – The second INCITS 378-2004 record, if used, contains 1 to 2 fingerprint templates
Iris	ISO/IEC 19794-6:2005 ▪ 0 to 2 CBEFF records, each containing 1 ISO/IEC 19794-6:2005 record – Each ISO/IEC 19794-6:2005 record contains 1 iris rectilinear image, compressed using a compression ratio no higher than 6:1	ISO/IEC 19794-6:2005 ▪ 0 to 2 CBEFF records, each containing 1 ISO/IEC 19794-6:2005 record – Each ISO/IEC 19794-6:2005 record contains 1 iris polar image, compressed – Compression ratio is arbitrary, provided resulting record fits within the specified iris container size on the RT card.
Face	INCITS 385-2004 ▪ 1 CBEFF record containing 1 INCITS 385-2004 record with 1 basic facial image – Compression ratio is arbitrary, provided resulting record fits within the specified facial container size on the RT card.	INCITS 385-2004 ▪ 1 CBEFF record containing 1 INCITS 385-2004 record with 1 basic facial image – The same facial image data collected at enrollment will be stored in the RT card, with no additional processing

Table 3-2. Biometric Data Formats

3.3.1 Data Format Standards

3.3.1.1 ANSI/NIST-ITL1-2000 (Biometric Data Interchange)

The American National Standards Institute (ANSI)/NIST standard “Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information” (ANSI/NIST-ITL 1-2000) defines the content, format, and units of measurement for electronically encoding and transmitting fingerprint, palm-print, facial/mugshot, and SMT images, and associated biographic information. Such information is intended for use in the interchange between criminal justice administrations or organizations that use an automated fingerprint and/or palm-print identification system, or use facial/mugshot or SMT data for identification purposes, providing a common messaging interface. The U.S. Department of Justice has defined an implementation (profile) of the ANSI/NIST-ITL 1-2000 standard, for use by law-enforcement agencies: the Electronic Fingerprint Transmission Specification (EFTS).

As indicated in Section 3.2.1.1, Fingerprint Enrollment, the Enrollment Provider will format fingerprint slap impressions using an XML representation of EFTS Type-14 records.

NOTE: The ANSI/NIST-ITL 1-2000 standard is currently undergoing its 5-year update and a new version is expected to be finalized in late 2006. The update may affect this technical specification. Because this technical specification is modeled on a draft of the new version, the impacts are expected to be minimal.

3.3.1.2 INCITS 378-2004 (Fingerprint Minutiae Data)

INCITS 378-2004 is the US national standard defining methods for representing fingerprint information using the concept of minutiae. It defines the placement of the minutiae on a fingerprint, a record format for containing the minutiae data, and optional extensions for ridge count and core/delta information. It was based on the American Association of Motor Vehicle Administrators (AAMVA) National Standard for Driver License/Identification Card 2000 and aligned where possible with the ANSI/NIST-ITL 1-2000 Type-9 record. It is intended to be used within a CBEFF-compliant structure in the CBEFF Biometric Data Block (BDB) as specified in INCITS 398-2005 (see Section 3.3.3.1, CBEFF). This standard applies to fingerprint templates, as opposed to fingerprint images, and allows processed fingerprint data to be exchanged. The basic INCITS 378-2004 format (with no extended data) consists of minutia type, location (X,Y in pixels), angle (in two degree increments), and quality (0-100).

INCITS 378-2004 is used in NIST SP 800-76, Biometric Data Specification for Personal Identity Verification, for representing fingerprint minutiae information. RT shall utilize the INCITS 378 Profile for PIV Card Templates as specified in NIST SP 800-76, Table 3. RT allows two to four fingerprint templates on the RT card, however NIST SP 800-76 allows only two. In applying the NIST SP 800-76 specification for the RT card, RT shall utilize one or two CBEFF records. The first CBEFF record shall contain one INCITS 378-2004 record with two fingerprint templates. The second CBEFF record, if used, shall contain one INCITS 378-2004 record with one or two fingerprint templates. Note that the CIMS will always attempt to generate four fingerprint templates. If the CIMS cannot generate four fingerprint templates (e.g., due to poor fingerprint quality or technical error), then the second CBEFF record will not be provided by CIMS.

3.3.1.3 ISO/IEC 19794-6:2005 (Iris Image Data)

ISO/IEC 19794-6:2005 specifies two alternative image interchange formats for biometric authentication systems that utilize iris recognition. The first is based on a rectilinear image storage format that may be a raw, uncompressed array of intensity values or a compressed format. The second format is based on a polar image specification that requires certain pre-processing steps, but produces a much more compact data structure that contains only iris information. Iris image data is intended to be embedded in a CBEFF-compliant structure in the CBEFF Biometric Data Block (BDB) as specified in INCITS 398-2005 (see Section 3.3.3.1, CBEFF).

Unlike the other standard data formats identified in this section, which are all US national standards, NIST SP 800-76, Biometric Data Specification for Personal Identity Verification, does not include a profile for iris image data. This provides RT with an opportunity to align with International Civil Aviation Organization (ICAO) standards for machine readable travel documents by selecting the international standard (ISO/IEC 19794-6) over the US national standard (INCITS 379). The two standards are very similar.

The primary intended use for iris data within the RT program is for verification of RT Participants at the verification station. For this purpose, iris enrollment data will be stored on the card in polar format to

assure compact data size and interoperability. Other potential uses exist, including checking for duplicate traveler enrollments, search of iris watch lists using data records presented for enrollment, and archival storage of iris enrollments to enable future technology upgrades.

In order to achieve the highest level of performance and interoperability, it is appropriate to specify a number of parameters and options that are defined in the ISO/IEC 19794-6:2005 standard. The RT system shall utilize ISO/IEC 19794-6:2005 as specified in Table 3-3 to represent iris images. Any data record values not listed in Table 3-3 are clearly defined in the base standard and no further specification is required. Rectilinear iris images shall be compressed using JPEG, with a compression ratio no higher than 6:1 in accordance with clause A.1.6 of ISO/IEC 19794-6:2005. The specification of format type is provided in the CBEFF header, which is described in Section 3.3.3.1, CBEFF. For the RT card, RT shall utilize up to two CBEFF records, each containing one ISO/IEC 19794-6:2005 record with one iris image in polar format. The polar iris image may be compressed using JPEG 2000, with a compression ratio that produces the best fit to the container on the RT card.

			Section title and/or field name (ISO/IEC 19794-6:2005 clause)	ISO/IEC 19794-6:2005		RT Conformance	Comments
				Field	Value	Values Allowed	
1.	CBEFF		CBEFF Header (6.1)	MF	MV	Based on Patron Format PIV	Multi-field CBEFF Header, as described in Section 3.3.3.1
2.	Iris Record Header		Format Identifier (6.5.1)	MF	MV	0x49495200	i.e., ASCII "IIR\0"
3.			Version Number (6.5.1)	MF	MV	0x30313000	i.e., ASCII "010\0"
4.			Record Length (6.5.1)	MF	MV	MIT	Size excluding CBEFF structure
5.			Capture Device ID (6.5.1)	MF	MV	MIT	Capture device ID assigned by vendor of equipment used to capture image data
6.			Number of iris biometric subtypes (6.5.1)	MF	MV	1	Only images from a single eye
7.			Record Header Length (6.5.1)	MF	MV	45	
8.		Iris Image Properties	Horizontal Orientation (6.5.1)	MF	MV	0 or 1	Horizontal orientation is correct
9.			Vertical Orientation (6.5.1)	MF	MV	0 or 1	Vertical orientation is correct
10.			Scan Type (6.5.1)	MF	MV	0	For rectilinear: scan type corrected For polar: not used
11.			Iris Occlusions (6.5.1)	MF	MV	0	For rectilinear: not used (0) For polar: occlusions not processed (0) [See Note 1.]
12.			Occlusion Filling (6.5.1)	MF	MV	0	For rectilinear: not used (0) For polar: zero fill (0) [See Note 1]
13.			Boundary Extraction (6.5.1)	MF	MV	0	For rectilinear: not used For polar: pupil and iris boundaries shall not be extracted
14.			Iris Diameter (6.5.1)	MF	MV	A	For rectilinear: iris diameter in pixels [See Note 2.] For polar: not used
15.			Image Format (6.5.1)	MF	MV	2, 6 or 14	For rectilinear monochrome: raw (2) or JPEG (6) For polar: monochrome: raw (2) or JPEG 2000 (14)
16.			Raw Image Width (6.5.1)	MF	MV	MIT	For rectilinear: image width in pixels For polar: 256 (number of angular samples)
17.			Raw Image Height (6.5.1)	MF	MV	MIT	For rectilinear: image height in pixels For polar: 64 (number of radial samples) [See Note 3]

			Section title and/or field name (ISO/IEC 19794-6:2005 clause)	ISO/IEC 19794-6:2005		RT Conformance	Comments
				Field	Value	Values Allowed	
18.			Intensity Depth (6.5.1)	MF	MV	8	Number of bits per pixel
19.			Image Transformation (6.5.1)	MF	MV	0 or 1	For rectilinear: not used For polar: standard transformation recommended but not mandatory
20.			Device Unique Identifier (6.5.1)	MF	MV	A	May be 0 to represent that no device unique identifier is identified
21.	Iris Subtype Header		Iris Subtype (6.5.2)	MF	MV	A	
22.			Number Images (6.5.2)	MF	MV	1	
23.	Iris Image Header		Image Number (6.5.3)	MF	MV	1	
24.			Quality (6.5.3)	MF	MV	61 ≤ N ≤ 100	Good quality for enrollment data [See Note 2.]
25.			Rotation Angle of Eye (6.5.3)	MF	MV	MIT	For rectilinear: rotation angle, else 0xFFFF if undefined For polar – 0xFFFF for undefined
26.			Rotation Uncertainty (6.5.3)	MF	MV	MIT	0xFFFF if undefined
27.			Image Length (6.5.3)	MF	MV	MIT	
28.			Iris Image Data	MF	MV	MIT	Rectilinear or polar iris image

Table 3-3. ISO/IEC 19794-6 Profile for RT Iris Images

Note 1: Occlusion processing is not used when JPEG2000 lossy compression is used. Any occlusion processing must therefore be done during the verification operation.

Note 2: A minimum iris diameter of 170 pixels is required, which corresponds (other quality factors not considered) to a minimum quality value of 61. Upsampling of images produced by the iris camera is prohibited.

Note 3: For polar images, 64 is a nominal value; the height of the image should ensure at least 32 pixels between the pupil boundary and the sclera boundary and at least a 4 pixel margin beyond the iris-sclera boundary.

Table 3-3 is modeled on the NIST SP 800-76 standard profiles. The following acronyms are used in the table:

- MF: Mandatory Field (ISO/IEC 19794-6:2005 requires the field to be present)
- MV: Mandatory Value (ISO/IEC 19794-6:2005 requires a meaningful value for the field)
- MIT: Mandatory at the time of Instantiation (For RT, mandatory value that shall be determined at the time the record is instantiated and shall follow the practice specified in ISO/IEC 19794-6:2005)
- A: As required (For RT, value or practice is as normatively specified in ISO/IEC 19794-6:2005).

3.3.1.4 INCITS 385-2004 (Facial Image Data)

INCITS 385-2004 defines an intermediate interchange format for the exchange of facial image data for both human and automated verification and identification. The face pattern record format is used to provide interoperability between uses of face recognition systems and digital face image storage systems. It defines the composition of the facial record pertaining to a single subject and may contain one or more images of a human face. This standard is intended to be used within a CBEFF-compliant structure in the CBEFF Biometric Data Block (BDB) as specified in INCITS 398-2005 (see Section 3.3.3.1, CBEFF).

The record structure includes a facial header and facial data, the latter consisting of facial information, feature points, image information, and image data. Another important element of this standard is the best practices for photo image capture found in the annexes.

DHS has adopted this standard as an official DHS standard and has licensed the copyright. INCITS 385-2004 is also used in NIST SP 800-76, Biometric Data Specification for Personal Identity Verification, for representing full frontal facial image information. Because facial recognition is not a requirement of the RT program, the basic facial image format of INCITS 385-2004 rather than the full frontal facial image format shall be used.

The RT system shall utilize INCITS 385-2004 as specified in Table 3-4 to represent facial image data. As stated in NIST SP 800-76 (Table 6, Note 5) the RT system also allows use of either JPEG 2000 or JPEG compression, though the former is preferred. The RT system adopts the recommendation in NIST SP 800-76 (Table 6, Note 6) regarding the use of region of interest compression; however no maximum compression ratios are specified for facial image data in order to best fit the image in the container defined for the card.

		Section title and/or field name (INCITS 385-2004 clause)	INCITS 385-2004		RT Conformance	Comments
			Field	Value	Values Allowed	
1.		Byte Ordering (5.2.1)	NC		A	Big Endian
2.		Numeric Values (5.2.2)	NC		A	Unsigned Integers
3.	CBEFF	CBEFF Header (5.3)	MF	MV	Based on Patron Format PIV	Multi-field CBEFF Header, as described in Section 3.3.3.1
4.	Facial Header	Format Identifier (5.4.1)	MF	MV	0x46414300	i.e., ASCII "FAC\0"
5.		Version Number (5.4.2)	MF	MV	0x30313000	i.e., ASCII "010\0" (Ver 1, Rev 0)
6.		Record Length (5.4.3)	MF	MV	MIT	Size excluding CBEFF structure
7.		Number of Facial Images (5.4.4)	MF	MV	1	
8.	Facial Information	Facial Image Block Length (5.5.1)	MF	MV	MIT	
9.		Number of Feature Points (5.5.2)	MF	MV	≥ 0	Positive, if features computed.
10.		Gender (5.5.3)	MF	OV	OIT	These fields populated with meaningful values at EP discretion, otherwise 0 for unspecified.
11.		Eye Color (5.5.4)	MF	OV	OIT	
12.		Hair Color (5.5.5)	MF	OV	OIT	
13.		Feature Mask (5.5.6)	MF	OV	OIT	
14.		Expression (5.5.7)	MF	OV	1	Neutral
15.		Pose Angles (5.5.8)	MF	OV	OIT	
16.		Pose Angle Uncertainty (5.5.9)	MF	OV	OIT	
17.	Features	MPEG4 Features (5.6.1)	NC		OIT	
18.		Center of Facial Features (5.6.2)	NC		OIT	
19.		The Facial Feature Block Encoding (5.6.3)	OF	OV	OIT	
20.	Image Information	Facial Image Type (5.7.1)	MF	MV	0	
21.		Image Data Type (5.7.2)	MF	MV	0 or 1	JPEG 2000 preferred.
22.		Width (5.7.3)	MF	MV	MIT	
23.		Height (5.7.4)	MF	MV	MIT	
24.		Image Color Space (5.7.5)	MF	MV	1	sRGB.
25.		Source Type (5.7.6)	MF	MV	2 or 6	Digital still or digital video

			Section title and/or field name (INCITS 385-2004 clause)	INCITS 385-2004		RT Conformance	Comments
				Field	Value	Values Allowed	
26.			Device Type (5.7.7)	MF	MV	MIT	May be 0 to represent that no device type is identified
27.			Quality (5.7.8)	MF	MV	0	INCITS 385 requires 0 (unspecified)
28.	Image Data		Data Structure (5.8.1)	MF	MV	MIT	Compressed Data
29.	Basic Face Image Type	Inheritance	Inheritance (6.1)	NC		A	
30.			Image Data Encoding (6.2)	NC		A	JPEG 2000 preferred
31.			Image Data Compression (6.3)	NC		A	
32.		Format	Facial Header (6.4.1)	NC		A	Include 4 fields
33.			Facial Information (6.4.2)	NC		A	Include 9 fields
34.			Image Information (6.4.3)	NC		A	Include 8 fields

Table 3-4. INCITS 385-2004 Profile for RT Facial Images

Table 3-4 is modeled on the INCITS 385-2004 Profile for PIV Facial Images in NIST SP 800-76 (Table 6). The following acronyms are used in the table:

- MF: Mandatory Field (INCITS 385-2004 requires the field to be present)
- MV: Mandatory Value (INCITS 385-2004 requires a meaningful value for the field)
- OF: Optional Field (INCITS 385-2004 allows the field to be present)
- OV: Optional Value (INCITS 385-2004 allows a meaningful value or allows 0 to be used to connote "unspecified")
- MIT: Mandatory at the time of Instantiation (For RT, mandatory value that shall be determined at the time the record is instantiated and shall follow the practice specified in INCITS 385-2004)
- OIT: Optional at the time of Instantiation (For RT, optional value that may be determined at the time the record is instantiated)
- NC: Normative content (INCITS 385-2004 gives normative practice for the RT program; such sections do not define a field in the facial image data record)
- A: As required (For RT, value or practice is as normatively specified in INCITS 385-2004).

3.3.2 Data Compression

3.3.2.1 WSQ Gray-Scale Fingerprint Image Compression

The Wavelet Scalar Quantization (WSQ) Gray-Scale Fingerprint Image Compression Algorithm is the standard for the exchange of fingerprint images within the criminal justice community. It specifies the class of encoders required for converting source fingerprint image data to compressed image data, the decoder process for converting compressed image data to reconstructed fingerprint image data, and the coded representations for compressed image data with minimal loss of information.

As required by EFTS, RT will compress fingerprint images using WSQ. Compression ratios shall be in accordance with EFTS requirements.

3.3.2.2 JPEG 2000

The JPEG 2000 Image Coding System is the latest series of standards (ISO/IEC 15444) from the JPEG committee (http://www.jpeg.org). JPEG 2000 uses wavelet technology to compress images, allowing an

image to be retained without any distortion or loss. Specifically, the series of standards define a set of lossless (bit-preserving) and lossy compression methods for coding continuous-tone, bi-level, grey-scale, or color digital still images. It specifies the encoding process for converting source image data to compressed image data, the decoding processes for converting compressed image data to reconstructed image data, and a file format for storing compressed image data.

As indicated in Section 3.3.1.3, ISO/IEC 19794-6:2005, and Section 3.3.1.4, INCITS 385-2004, the RT system may use JPEG 2000 for polar iris image and facial image data compression.

3.3.2.3 JPEG

JPEG refers to the international standard ("Digital Compression and Coding of Continuous-Tone Still Images," ISO/IEC 10918) from the JPEG committee that defines the method for compressing still images of photographic quality. JPEG is designed for compressing either full-color or gray-scale images of natural, real-world scenes. It works well on photographs, naturalistic artwork, and similar material; not so well on lettering, simple cartoons, or line drawings. JPEG handles only still images. The JPEG File Interchange Format (JFIF) specifies a file format that enables the exchange of JPEG compressed images.

As indicated in Section 3.3.1.3, ISO/IEC 19794-6, the RT system will use JPEG for rectilinear iris image compression. The maximum allowed compression ratios for rectilinear iris image compression are also specified in Section 3.3.1.3, ISO/IEC 19794-6. As indicated in Section 3.3.1.4, INCITS 385-2004, the RT system may use JPEG for facial image data compression. Note that JPEG 2000 is the preferred compression algorithm for facial image data.

3.3.3 Other Related Standards

3.3.3.1 CBEFF

The Common Biometric Exchange Formats Framework (CBEFF) is described in INCITS 398-2005. CBEFF describes a set of data elements necessary to support biometric technologies in a common way. These data can be placed in a single file used to exchange biometric information between different system components or between systems. The result promotes interoperability of biometric-based application programs and systems developed by different vendors by allowing biometric data interchange.

CBEFF describes a set of "Required" and "Optional" fields, a "Domain of Use" to establish the applicability of a standard or specification that meets CBEFF requirements, and a process by which new technology or systems can create formats that meet these requirements. CBEFF allows for these standards or specifications to define a format and for these formats to define the data encoding. CBEFF patrons are organizations that have the authority to define and publish CBEFF patron formats; patron formats specify what CBEFF fields are used in a particular domain of use.

The RT system shall use the CBEFF PIV patron format identified in NIST SP 800-76, Biometric Data Specification for Personal Identity Verification, tailored for RT as described in Table 3-5. The PIV Patron Format specifies the use of the CBEFF signature block; however, this layer of security is redundant with security layers already on the card. Therefore, the RT system shall not use the CBEFF signature block.

Field	Size (bytes)	Value
Patron Header Version	1	0x03
SBH Security Options	1	0x00
BDB Length	4	Length, in bytes, of the biometric data
SB Length	2	0x0000
BDB Format Owner	2	For fingerprint and facial data: 0x001B For iris data: 0x0101
BDB Format Type	2	For fingerprint templates: 0x0201 For facial images: 0x0501 For iris images: 0x0009 (rectilinear), 0x000B (polar)
Biometric Creation Date	8	See Note 1.
Validity Period	16	0x00000000 00000000 00000000 00000000 (spaces added for readability)
Biometric Type	3	Fingerprints: 0x000008 Face: 0x000002 Iris: 0x000010
Biometric Data Type (See Note 2)	1	Fingerprint, Face, and Iris Images: b001xxxxx (raw) Fingerprint Templates: b100xxxxx (processed)
Biometric Data Quality	1	Fingerprints: 20*(6 - NFIQ) [See Note 3.] Face: -2 Iris: a value ≥ 61 and ≤ 100
Creator	18	Text string identifying the Enrollment Provider or CIMS, as applicable
FASC-N	25	0x00000000 00000000 00000000 00000000 00000000 00000000 00 (spaces added for readability)
Reserved for Future Use	4	0x00000000

Table 3-5. PIV Patron Format (Tailored to RT)

Note 1: This is the date that the biometric sample was acquired. For processed samples (e.g., templates) this data should be the date of acquisition of the parent sample. Creation Date shall be encoded in eight bytes using a binary representation of "YYYYMMDDhhmmssZ". Each pair of characters (for example, "DD") is coded in 8 bits as an unsigned integer. Thus 17:35:30 December 15, 2005 is represented as: 00010100 00000101 00001100 00001111 00010001 00100011 00011110 01011010 where the last byte is the binary representation of the ASCII character Z which is included to indicate that the time is represented in Coordinated Universal Time (UTC). The field "hh" shall code a 24 hour clock value. If no acquisition time is available (i.e., the Type-14 or Type-99 enrollment record contains date, but not time), then the time fields (hhmmss) shall be set to all zeros (000000).

Note 2: The biometric data type field and corresponding values are described in INCITS 398-2005. In this context, a value of "raw" applies to either uncompressed or compressed images.

Note 3: When the INCITS 378 record contains two fingerprint templates, the quality value in the CBEFF header is determined by taking the better of the two quality values (lower NFIQ, higher CBEFF biometric data quality).

3.3.3.2 NISTIR 7151

The NIST Fingerprint Image Quality (NFIQ) value is a prediction of a matcher's performance, reflecting the positive or negative contribution of an individual sample to the overall performance of a fingerprint matching system. It consists of five levels of quality related to the performance of a minutiae-based fingerprint matching system. An NFIQ value of 1 indicates high quality samples and a value of 5 indicates poor sample quality.

The NIST NFIQ algorithm performs a feature extraction operation followed by neural network processing which assesses the quality based on a normalized score distribution. It has been shown to accurately predict matching performance across a variety of datasets and matching algorithms. NFIQ is publicly available, subject to export restrictions.

As indicated in Section 3.2.1.1, Fingerprint Enrollment, and as required by EFTS, the RT system will use NFIQ to assess fingerprint image quality. NFIQ values of 1, 2, or 3 are acceptable quality scores for RT.

4 System Messaging

This section provides details on the data content and format that is interchanged between SPs and the CIMS. Where only specific data items apply, the interface is fully contained within an SP's domain, only the specification of these data items is given. The goal is to avoid forcing formats and rigorous specifications on activities that remain within an SP's domain. However, communication between actors, including the CIMS, must have rigorous definition to ensure interoperability.

4.1 Communication Architecture

To ensure a simplified yet consistent data interchange between SPs, the Java Messaging System (JMS) Specification 1.0.2 will be used. All SPs must implement a JMS-compliant message queuing server to receive messages from the CIMS or other SPs. Most current message queuing implementations on the market at this time support JMS; thus, this is not perceived as a significant impact to new SPs. Using message queuing (MQ) capabilities provides a stronger level of data interchange between SPs, allowing the MQ server to manage message delivery rather than the application having to implement off-nominal conditions. Some of the benefits of MQ are guaranteed delivery, retry/resend, delivery receipts, and broadcast support. By using MQ servers, SPs do not have to poll for data or status. As soon as information is available, it can be "pushed" to the destination. This allows for a more timely response to system events. If messages must be separated into smaller pieces due to message size limits, MQ servers provide a transactional capability that supports "all or none" delivery. Transactional messages that are expected to become extremely large will include a sequence element to identify the order of messages.

For security purposes, all message interchange will occur over secure session (SSL/TLS) communication channels. When "sensitive" message content is involved, that content will be encrypted with a session symmetric key and will be encrypted with an asymmetric key that allows only the intended recipient to decrypt and view the content. In this way, secure session communication over the Internet can be achieved. Please refer to Section 6, System Security, for more information.

4.2 Message Structure

This section defines the overall internal structure of all messages traversing the boundary lines of the domains defined in this interoperability specification. This structure conforms with security and traceability requirements imposed by the government and the RTIC. While this document does not govern the SP's internal communications, the RTIC recommends that the SPs adopt this specification for that purpose as well. If an SP chooses to develop a different messaging architecture, the SP should refer to the other sections of this document to ensure government requirements will be satisfied.

Messages within the RT program that are used for interchange between SPs, including the CIMS, will be XML-based. Some content that the SP must support will be defined using an XML schema but the actual means by which the SP manages the content is not specified here. The intent is to allow the SP full control over how data is moved within the SP's system and only require specification for data that must be transmitted outside the SP's purview.

The root tag of all messages transmitted between SPs and the CIMS will be "RTMSG." There will be two primary elements within the message, "Header" and "Content." All messages have the same header fields but content fields are dependent on the message itself. The use of XML attributes have been minimized to simplify parsing. Sub-element XML tags have been defined to detail data items that relate to the outer tag.

4.2.1 Namespace for RT messages

The namespace for the RT program messages will be as shown below:

```
xmlns="http://www.rtconsortium.org/2006/06/TBD"
```

The date that is part of this namespace allows use of the namespace as a versioning of the message definitions. Future specifications can determine if a new namespace is used to affect all message definitions or if only parts of messages are affected. The actual namespace to be used and the XML schema will be made available to SPs at a later time.

4.2.2 Example RT Message

The following is an example message used during card re-issuance and is sent from the EP to request a new card for an RT Applicant:

```
[01]  <RTMSG xmlns="http://www.rtconsortium.org/2006/06/TBD"
         version="1.0" >
[02]    <Header>
[03]      <MessageType>EPCHCardReissuanceRequest</MessageType>
[04]      <SPID>AA</SPID>
[05]      <RTCN>0123456789000</RTCN>
[05A]     <ProcessingGroup>RTPART</ProcessingGroup>
[06]      <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
[07]        <SignedInfo>
[08]          <CanonicalizationMethod
                Algorithm="http://www.w3.org/TR/2001/
                REC-xml-c14n-20010315"/>
[09]          <SignatureMethod
                Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
[10]          <Reference URI="//Content">
[11]            <DigestMethod
                  Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
[12]            <DigestValue>base64+content</DigestValue>
[13]          </Reference>
[14]        </SignedInfo>
[15]        <SignatureValue>base64+content</SignatureValue>
[16]      </Signature>
[17]    </Header>
[18]    <Content>
[19]      <EPCHCardReissuanceRequest>
[20]        <RTID>1234567890ABCDEF</RTID>
[21]        <RequestedFingers>2,3,6,7</RequestedFingers>
[22]      </EPCHCardReissuanceRequest>
[23]    </Content>
[24]  </RTMSG>
```

In this example, line [01] provides the root tag for a registered traveler message and identifies the version through use of the namespace. Line [02] begins the header which contains the message type (line [03]), the SPID (line [04]), the RTCN (line [05]), the processing group (line[05A]), and the message digital signature (lines [06]-[16]). Notice that line [10] denotes the signature is over the full content element (lines [18]-[23]) through the use of the XPath specification "//Content." The body of the message is given as the content consisting of a single element, the message type, in this case "EPCHCardReissuanceRequest" (line [19]). This message contains two child elements (lines [20]-[21]), as shown, which are detailed in Section 4.9.1, EPCH Card Re-issuance Request.

The RT message schema is given here and consists of only two elements, both of which are described in further detail below:

```
<xs:complexType name=”RTMsgType”>
  <xs:sequence>
    <xs:element name=”Header” type=”RTHeaderType”/>
    <xs:element name=”Content” type=”RTContentType”/>
  </xs:sequence>
</xs:complexType>
```

4.2.3 Message Header

All RT messages that are transferred between SPs and the CIMS must contain a message header that contains four elements and a digital signature of the message which can be used for authentication.

The schema for the message header shows these two elements where “ds:Signature” is the W3C digital signature as defined by http://www.w3.org/2000/09/xmldsig and http://www.w3.org/TR/xmldsig-core/.

```
<xs:complexType name=”RTHeaderType”>
  <xs:sequence>
    <xs:element name=”MessageType” type=”MessageContentType”/>
    <xs:element name=”SPID” type=”SPIDType”/>
    <xs:element name=”RTCN” type=”ControlNumberType”/>
    <xs:element name=”RTCR” type=”ControlNumberType” minOccurs=”0”>
    <xs:element name="ProcessingGroup" type="ProcessingGroupType"/>
    <xs:element ref=”ds:Signature” />
  </xs:sequence>
</xs:complexType>
```

<MessageType> identifies the type of message which contains the same value that is used in the <Content> element.

<SPID> provides the Service Provider ID that is sending the message.

<RTCN> provides the RT Control Number from the message sender. This number must be returned in the <RTCR> element for messages that require a response.

<RTCR> provides the RT Control Reference Number. This number returns the value of the <RTCN> that was sent in the previous message in the workflow between organizations.

The following is an example message header:

```
<Header>
  <MessageType>EPCHCardReissuanceRequest</MessageType>
  <SPID>AA</SPID>
  <RTCN>00030</RTCN>
  <ProcessingGroup>RTPART</ProcessingGroup>
  <Signature xmlns=”http://www.w3.org/2000/09/xmldsig#”>
    <SignedInfo>
      <CanonicalizationMethod
          Algorithm=”http://www.w3.org/TR/2001/REC-xml-c14n-20010315”/>
      <SignatureMethod
          Algorithm=”http://www.w3.org/2000/09/xmldsig#dsa-sha1”/>
      <Reference URI=”//Content”>
        <DigestMethod
            Algorithm=”http://www.w3.org/2000/09/xmldsig#sha1”/>
        <DigestValue>base64+content</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>base64+content</SignatureValue>
  </Signature>
```



```
</Header>
```

4.2.4 Message Type

To enhance the workflows for messaging, the Message Type in the Message Content will also be supplied in the header. This enumerated value matches the Message Content type. The schema for the message content type shows the various message types that are sent in the Message Content.

```
<xs:simpleType name="MessageContentType">
  <xs:restriction base="xs:string">
    <xs:enumeration value="CHEPCardReissuanceResponse"/>
    <xs:enumeration value="CHEPEnrollmentResponse"/>
    <xs:enumeration value="CHEPRevocationResponse"/>
    <xs:enumeration value="CHEPRevocationRequest"/>
    <xs:enumeration value="CHVPHotListResponse"/>
    <xs:enumeration value="EPCHActiveApplicantNotification"/>
    <xs:enumeration value="EPCHCardRequestConfirmation"/>
    <xs:enumeration value="EPCHCardReissuanceRequest"/>
    <xs:enumeration value="EPCHEnrollmentConfirmation"/>
    <xs:enumeration value="EPCHEnrollmentRequest"/>
    <xs:enumeration value="EPCHRevocationResponse"/>
    <xs:enumeration value="EPCHRevocationRequest"/>
    <xs:enumeration value="VPCHHotListRequest"/>
    <xs:enumeration value="VPCHVerficationEvent"/>
    <xs:enumeration value="VPEPVerificationEvent"/>
  </xs:restriction>
</xs:simpleType>
```

4.2.5 Message Content

There are two forms of message content, plain (unencrypted), and encrypted. Plain form consists of XML-based content, as shown below, while encrypted form is based on W3C XML-encryption standard as defined by http://www.w3.org/2001/04/xmlenc and http://www.w3.org/TR/xmlenc-core/. When encryption is used, the “XML element content” encryption form of the Content element is encrypted. The <Content> tags will be plain text and the message tags will be encrypted with the data.

The schema for the message content shows the various message types that can exist and are described further throughout the full message document.

```
<xs:complexType name=”RTContentType”>
  <xs:choice>
    <xs:element ref="CHEPCardReissuanceResponse"/>
    <xs:element ref="CHEPEnrollmentResponse"/>
    <xs:element ref="CHEPRevocationResponse"/>
    <xs:element ref="CHEPRevocationRequest"/>
    <xs:element ref="CHVPHotListResponse"/>
    <xs:element ref="EPCHActiveApplicantNotification"/>
    <xs:element ref="EPCHCardRequestConfirmation"/>
    <xs:element ref="EPCHCardReissuanceRequest"/>
    <xs:element ref="EPCHEnrollmentConfirmation"/>
    <xs:element ref="EPCHEnrollmentRequest"/>
    <xs:element ref="EPCHRevocationResponse"/>
    <xs:element ref="EPCHRevocationRequest"/>
    <xs:element ref="VPCHHotListRequest"/>
    <xs:element ref="VPCHVerficationEvent"/>
    <xs:element ref="VPEPVerificationEvent"/>
  </xs:choice>
```

```
</xs:complexType>
```

This example is of the “EPCHCardReissuanceRequest” (card re-issuance request) message and the content is defined by the message itself with the “<EPCHCardReissuanceRequest>” tags.

The naming convention for message names begins with a four character message name with the first two characters for the sending organization, the second two characters for the receiving organization, and a message type. The “<EPCHCardReissuanceRequest>” tag represents an EP to CIMS (where CH represents the CIMS) card re-issuance request.

```
<Content>
  <EPCHCardReissuanceRequest>
    <RTID>A1B2C3D4E5F6G7H8</RTID>
    <RequestedFingers>2,3,6,7</RequestedFingers>
  </EPCHCardReissuanceRequest>
</Content>
```

4.3 Common Message Elements

This section provides message elements that may be used in more than one message. These are typically common XML types used throughout the document. Examples here are generally small and may include XML tags from other messages.

4.3.1 Service Provider ID

All SPs within the RT program are assigned a two character unique identifier by the TSC. The SPID, which is transmitted in the header of all messages, contains this two character identifier allowing use by all recipients of the message to ensure the SP is recognized and, through use of the message’s digital signature, validate message authentication. The XML definition for the SPID is:

```
<xs:simpleType name=”SPIDType”>
  <xs:restriction base=”xs:token”>
    <xs:length value=”2” fixed=”true” />
    <xs:pattern value=”[A-Z0-9][A-Z0-9]”/>
  </xs:restriction>
</xs:simpleType>
```

The following example shows a possible SPID:

```
<SPID>AA</SPID>
```

4.3.2 Identifier

An “identifier” is a fixed-length 16-character string consisting only of uppercase alphanumeric characters, the “_” (underscore) character, and the “-“ (hyphen) character that is used for identification (e.g., RT Participant accounts).

The XML definition for an identifier that specifies the fully qualified pattern expression is shown below:

```
<xs:simpleType name=”IdentifierType”>
  <xs:restriction base=”xs:token”>
    <xs:length value=”16” fixed=”true” />
    <xs:pattern value=”[A-Z0-9_\-]{16}”/>
  </xs:restriction>
</xs:simpleType>
```

The following example shows a possible RTID:

```
<RTID>A1B2-C3D4E5_F6G7</RTID>
```


4.3.3 Control Number

To enhance workflow between organizations, a control number has been included in the message headers. The XML definition for a Control Number is shown below:

```
<xs:simpleType name="ControlNumberType">
  <xs:restriction base="xs:string">

    <xs:maxLength value="50" />
  </xs:restriction>
</xs:simpleType>
```

4.3.4 ADSN (Authentication Data Sequence Number)

To ensure each RT card issued contains a unique identifier, a combination of SPID, RTID, and ADSN is used. The ADSN is a single character consisting of a digit or uppercase letter generated by the CIMS and provided with the authentication payload when a card is issued. The limit of 36 unique values is sufficient for a single RT Participant. The XML definition for an ADSNType is shown below:

```
<xs:simpleType name=”ADSNType”>
  <xs:restriction base=”xs:token”>
    <xs:length value=”1” fixed=”true” />
    <xs:pattern value=”[0-9A-Z]”/>
  </xs:restriction>
</xs:simpleType>
```

The following example shows a possible ADSN:

```
<ADSN>2</ADSN>
```

4.3.5 Applicant State

The applicant state provides a machine readable value that denotes the current status of an application as specified within the active applicant list, Section 4.8, Active Applicant Consistency Check. The following values are defined for this type:

- ACTIVE: denotes an active applicant with a valid card.
- PENDING: denotes an applicant pending TSA STA with no card yet issued.
- CANCELED: denotes an applicant who has canceled membership with the EP.
- EXPIRED: denotes an applicant with an expired account which has not yet been removed from the list due to not having exceeded the 90 day period for removal.
- SUSPEND: denotes an applicant with a card that is presently in a suspended state.
- TSA_REVOKED_RTP: denotes an applicant which has been revoked by the TSA.
- TSA_SUSPEND_RTP: denotes an applicant which has been suspended by the TSA.
- TSA_REVOKED_SP: denotes an SP which has been revoked by the TSA.
- TSA_SUSPEND_SP: denotes an SP which has been suspended by the TSA.

The XML definition for this type is shown below:

```
<xs:simpleType name=”ApplicantStateType”>
  <xs:restriction base=”xs:string”>
    <xs:enumeration value=”ACTIVE”/>
    <xs:enumeration value=”PENDING”/>
    <xs:enumeration value=”CANCELLED”/>
    <xs:enumeration value=”EXPIRED”/>
    <xs:enumeration value=”SUSPEND”/>
```



```
      <xs:enumeration value="TSA_REVOKED_RTP"/>
      <xs:enumeration value="TSA_SUSPEND_RTP"/>
      <xs:enumeration value="TSA_REVOKED_SP"/>
      <xs:enumeration value="TSA_SUSPEND_SP"/>
    </xs:restriction>
  </xs:simpleType>
```

The following two examples show possible uses of the applicant state:

```
<State>ACTIVE</State>
<State>EXPIRED</State>
```

4.3.6 Revocation Action

The revocation action provides a reason why an RT Participant's card or the RT Participant is being revoked. The values are defined for this field:

- NONE: no action taken (used as action response on failure conditions).
- REPLACED: card is being replaced (lost/stolen, error, damaged, etc).
- CANCELED: RT Participant has canceled membership with the EP.
- EXPIRED: RT Participant's account has expired and was not renewed.
- SUSPEND: EP is requesting the RT Participant's card be suspended.
- RESTORE: EP is requesting the RT Participant's card be restored.
- TSA_REVOKED_RTP: the TSA has revoked the RT Participant.
- TSA_SUSPEND_RTP: the TSA has suspended the RT Participant.
- TSA_RESTORE_RTP: the TSA is restoring the RT Participant.
- TSA_REVOKED_SP: the TSA has revoked the SP.
- TSA_SUSPEND_SP: the TSA has suspended the SP.
- TSA_RESTORE_SP: the TSA is restoring the SP.
- SP_REMOVE_OFFICER: the SP is removing an officer.
- SP_REMOVE_EMPLOYEE: the SP is removing an employee.

The XML definition for this type is shown below:

```
<xs:simpleType name="RevokeActionType">
  <xs:restriction base="xs:string">
    <xs:enumeration value="NONE"/>
    <xs:enumeration value="REPLACED"/>
    <xs:enumeration value="CANCELED"/>
    <xs:enumeration value="EXPIRED"/>
    <xs:enumeration value="SUSPEND"/>
    <xs:enumeration value="RESTORE"/>
    <xs:enumeration value="TSA_REVOKED_RTP"/>
    <xs:enumeration value="TSA_SUSPEND_RTP"/>
    <xs:enumeration value="TSA_RESTORE_RTP"/>
    <xs:enumeration value="TSA_REVOKED_SP"/>
    <xs:enumeration value="TSA_SUSPEND_SP"/>
    <xs:enumeration value="TSA_RESTORE_SP"/>
    <xs:enumeration value="SP_REMOVE_OFFICER"/>
    <xs:enumeration value="SP_REMOVE_EMPLOYEE"/>
  </xs:restriction>
</xs:simpleType>
```

The following example shows a possible use of the revocation action:

```
<Action>CANCELED</Action>
```


4.3.7 Authentication Payload

The Authentication Payload, AuthPayloadType, consists of the fields that must be placed on the card. These are the items which must be written to the card without change. This data is signed by the CIMS and then provided to the EP for card issuance.

The schema definition for this message content consists of the following elements:

```
<xs:complexType name=”AuthPayloadType”>
  <xs:sequence>
    <xs:element name=”FingerprintObjectOne” type=”xs:base64Binary” />
    <xs:element name=”FingerprintObjectTwo” type=”xs:base64Binary” />
    <xs:element name=”IrisObject” type=”xs:base64Binary” />
    <xs:element name="FacialObject" type="xs:base64Binary" />
    <xs:element name=”PersonalDataObject” type=”xs:base64Binary” />
    <xs:element name=”SecurityDataAuthObject” type=”xs:base64Binary” />
    <xs:element name=”CardKey” type=”xs:base64Binary” />
    <xs:element name=”KeyVersion” type=”xs:string” />
  </xs:sequence>
</xs:complexType>
```

<FingerprintObjectOne> provides a CBEFF record containing one INCITS 378-2004 record. This value is defined in Section 3.3, Biometrics Formats and Standards.

<FingerprintObjectTwo> provides a CBEFF record containing one INCITS 378-2004 record. This value is defined in Section 3.3, Biometrics Formats and Standards.

<IrisObject> provides up to two CBEFF records containing one ISO/IEC 19794-6:2005 record. Although iris data is not required the object structure must be created for the security object. This value is defined in Section 3.3, Biometrics Formats and Standards.

<FacialObject> provides a Facial Image record containing one INCITS 385-2004 record with CBEFF header. This value is defined in Section 3.3, Biometrics Formats and Standards.

<PersonalDataObject> contains fields including the order in which biometrics are stored in the containers. The biometric mapping contains identifiers for each biometric.

<SecurityDataAuthObject> contains the group signature of hashes of all other data objects.

<CardKey> provides the derived key (KC) for the card based on the derivation data and the master key (KM).

<KeyVersion> provides the version of the KM that was used to create the KC.

An example of an authentication payload consists primarily of base64-encoded content, but the tag structure would appear similar to the following:

```
<Payload>
  <FingerprintObjectOne>base64+content</FingerprintObjectOne>
  <FingerprintObjectTwo>base64+content</FingerprintObjectTwo>
  <IrisObject>base64+content</IrisObject>
  <FacialObject>base64+content</FacialObject>
  <PersonalDataObject>base64+content</PersonalDataObject>
  <SecurityDataAuthObject>base64+content</SecurityDataAuthObject>
  <CardKey>base64+content</CardKey>
  <KeyVersion>1</KeyVersion>
</Payload>
```


4.3.8 Enrollment Data

The US Department of Justice has defined an implementation (profile) of the ANSI/NIST-ITL 1-2000 standard for use by law-enforcement agencies. This implementation, the Electronic Fingerprint Transmission Specification (EFTS), is used worldwide for exchanging and storing rolled and flat fingerprint images. It is used not only by law-enforcement agencies, but also in many civilian identity systems. EFTS is also presently required for the FBI's Integrated Automated Fingerprint Identification System (IAFIS).

Due to its broad acceptance across industry, especially with regard to interchanging 10-print fingerprint information, the RTIC is basing its biometric enrollment data on the ANSI/NIST-ITL 1-2000 including the changes approved in December 2005. Specifically, the changes that the RTIC will use are the new CBEFF record type and the XML representation of the standard (a draft of which is defined at http:///www.doj.state.wi.us/les/NIST-ITL/index.htm).

The RTIC Enrollment Data messages will use the following record types:

- Type-2 – Biographic and user defined descriptive text.
- Type-14 – Variable-resolution 10-print image records including fingerprint slaps and segmentation coordinates.
- Type-99 –
  - INCITS 385-2004 Face Recognition Format for Data Interchange
    - One facial image
  - ISO/IEC 19794-6:2005 Biometric data interchange formats - Part 6: Iris image data

```
<xs:complexType name="NIST-ITLBiometricInformationExchangePackageType">
  <xs:complexContent>
    <xs:extension base="j:SuperType">
      <xs:sequence>
        <xs:element ref="ITLUserDefinedDescriptiveTextRecord"/>
        <xs:element
            ref="nist-finger:
            ITLVariableResolutionFingerprintImageRecord"
            minOccurs="0" maxOccurs="3"/>
        <xs:element ref="nist-cbeff:ITL-CBEFFBiometricDataRecord"
            minOccurs="0" maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>
```

4.3.8.1 Type 2: Biographics and User Defined Descriptive Text

The person schema was defined using the Global JXDM Schema, http://justicexml.gtri.gatech.edu/subset_tool.html. The following elements have been chosen. Elements marked with an (R) are required.

- Last name (<PersonSurName> (R)): A last name or family name of a person.
- First name (<PersonGivenName> (R)): A first name of a person.
- Middle name (<PersonMiddleName> (R)): A middle name or initial of a person.

- Other names used (<PersonAlternateName>): An alternate name used by a person. Sometimes referred to as “AKA.”
- Gender (<PersonSexCode> (R)): The gender or sex of a person.
- Current home address (<LocationStreet>): The actual value of the address is reported in a <StreetFullText> sub-element.
- Current home city (<LocationCityName>): A name of a city or town.
- Current home state (<LocationStateCode.USPostalService>): A code identifying a state.
- Current home Zip code (<LocationPostalCodeID>): A Zip code or postal code. The actual value of the number is reported in an <ID> sub-element.
- Current home country (<LocationCountryCode.fips10-4>): A code that identifies a country, territory, or dependency.
- Current primary phone number (<ContactTelephoneNumber>): A primary phone number. The actual value of the number is reported in a <TelephoneNumberFullID> sub-element.
- Current secondary phone number (<ContactTelephoneNumber>): A secondary phone number. The actual value of the number is reported in a <TelephoneNumberFullID> sub-element.
- Current e-mail address (<ContactEmailID>): The actual value of the number is reported in an <ID> sub-element.
- Name of employer (<EmploymentEmployerName>): A name of an employer.
- Address of employer (<StreetFullText>): A complete street reference, e.g., "123 Main Street NW."
- Current employer city (<LocationCityName>): A name of a city or town.
- Current employer state (<LocationStateCode.USPostalService>): A code identifying a state.
- Current employer Zip code (<LocationPostalCodeID>): A Zip code or postal code. This element contains the five or nine digit zip code or foreign postal code for this location. The actual value of the number is reported in an <ID> sub-element.
- Current employer Country (<LocationCountryCode.fips10-4>): A code that identifies a country, territory or dependency.
- Date of birth (<PersonBirthDate> (R)): The date a person was born.
- Place of birth (<PersonBirthLocation> (R)): The place of birth. The actual value of the location is reported in a <LocationName > sub-element.
    - Note: This field must be present, but may be filled with “Not Available” if information is not provided by the traveler.
- US citizenship status (<PersonCitizenshipCode.fips10-4> (R)): A code identifying a country that assigns rights, duties, and privileges to a person due to the person's birth or naturalization in that country.
- Alien registration number (<PersonNationalID>) and arrival date (<IDEffectiveDate>) in US (if applicable).

- Height (<PersonHeightMeasure>): A measurement of the height of a person.
- Driver's license number (<DriverAuthorizationID.Detailed>): A driver license number. The actual value of the number is reported in an <ID> sub-element. The state of issuance is included in the <IDJurisdictionCode.ncicLIS> sub-element.
- Social Security Number (<PersonSSNID>): Optional. A Social Security Number for a person. Sometimes referred to as an SSN. The actual value of the number is reported in an <ID> sub-element.
- Previous home addresses (<LocationContactInformation>): Previous home addresses for the past five years.
- Documents (<RTDocument>): Enrollment documents. Each <RTDocument> element contains a document type (<DocumentTitle>) and a document (<Document>) sequence (<DocumentSequenceID>), document title (<DocumentTitleText>), document descriptive data (<DocumentDescriptionText>, disputed information (<DocumentDisputedReasonText>), and the document binary (<BinaryObject.Base64>).
    - Enumerated document titles include the following:
        - US_PASSPORT
        - FOREIGN_PASSPORT_UNEXPIRED
        - US_MILITARY_ID_OR_FORM214
        - STATE_ISSUED_DRIVER_LICENSE_OR_ID
        - CERT_BIRTH_ABROAD_FORM545_OR_FORM1350
        - ORIGINAL_OR_CERT_COPY_OF_US_BIRTH_CERTIFICATE
        - VALID_US_PRCARD_OR_ALIEN_REGCARD_WITH_PHOTO
        - CERT_OF_NATURALIZATION_FORMN550_OR_FORMN570
        - CERT_OF_CITIZENSHIP_FORMN560_OR_FORMN561
        - OTHER
- Image capture device (<ImageCaptureDevice> (R)): Identification information about the device used to capture the fingerprint images contained in the subsequent Type-14 records. Contains a sequence: capture device make (<CaptureDeviceMakeText>): Make (manufacturer) of the fingerprint capture device, capture device model (<CaptureDeviceModelText>): model of the fingerprint capture device, and capture device serial number (<CaptureDeviceSerialNumberText>): Serial number of the fingerprint capture device.
    - Note: All three subfields must be present; however, the serial number element may contain "UNKNOWN" if the serial number is not available.

This example is of a person described as the following:

- Male
- Six feet, two inches, in height
- Social Security Number is 123-45-6789

- Born in the District of Columbia on July 4th, 1967
- DC license number TT123-45-222
- Missing right middle finger
- Lives at 1 Main Street, Washington, DC 20002
- Works at 1600 Pennsylvania Avenue, NW, Washington, DC 20002
- Provided documents were a US Passport and an ID Card.

```
<ITLUserDefinedDescriptiveTextRecord>
<ImageDesignationCharacter>00</ImageDesignationCharacter>
<UserDefinedDescriptiveText>
    <OtherDescriptiveText>
      <Person>
        <PersonName>
          <PersonGivenName>John</PersonGivenName>
          <PersonMiddleName>E</PersonMiddleName>
          <PersonSurName>Doe</PersonSurName>
        </PersonName>
        <PersonAlternateName>
          <PersonGivenName>Jim</PersonGivenName>
          <PersonMiddleName>E</PersonMiddleName>
          <PersonSurName>Doe</PersonSurName>
        </PersonAlternateName>
        <PersonAlternateName>
          <PersonGivenName>Jim</PersonGivenName>
          <PersonMiddleName>M</PersonMiddleName>
          <PersonSurName>Doe</PersonSurName>
        </PersonAlternateName>
        <PrimaryContactInformation>
          <ContactTelephoneNumber>
            <TelephoneNumberFullID>571-555-1212</TelephoneNumberFullID>
          </ContactTelephoneNumber>
          <ContactTelephoneNumber>
            <TelephoneNumberFullID>202-555-1212</TelephoneNumberFullID>
          </ContactTelephoneNumber>
          <ContactEmailID>
            <ID>john.doe@mail.com</ID>
          </ContactEmailID>
          <ContactMailingAddress>
            <LocationStreet>
              <StreetFullText>1 Main Street</StreetFullText>
            </LocationStreet>
            <LocationCityName>Washington</LocationCityName>
            <LocationStateCode.USPostalService>DC
                 </LocationStateCode.USPostalService>
            <LocationPostalCodeID>
              <ID>20002</ID>
            </LocationPostalCodeID>
            <LocationCountryCode.fips10-4>US
                </LocationCountryCode.fips10-4>
          </ContactMailingAddress>
          <ContactMailingAddress>
            <LocationStreet>
              <StreetFullText>1 Previous Main Street</StreetFullText>
```



```
      </LocationStreet>
      <LocationCityName>Washington</LocationCityName>
      <LocationStateCode.USPostalService>DC
           </LocationStateCode.USPostalService>
      <LocationPostalCodeID>
        <ID>20002</ID>
      </LocationPostalCodeID>
      <LocationCountryCode.fips10-4>US
          </LocationCountryCode.fips10-4>
    </ContactMailingAddress>
  </PrimaryContactInformation>
  <PersonAssignedIDDetails>
    <PersonSSNID>
      <ID>123456789</ID>
    </PersonSSNID>
    <PersonLicenseID>
      <ID>String</ID>
      <IDEffectiveDate>1967-08-13</IDEffectiveDate>
    </PersonLicenseID>
    <PersonNationalID>
      <ID>A00-000-000</ID>
      <IDEffectiveDate>2006-01-31</IDEffectiveDate>
    <PersonNationalID>
  </PersonAssignedIDDetails>
  <PersonBirthDate>1967-07-04</PersonBirthDate>
  <PersonBirthLocation>
    <LocationName>DC</LocationName>
  </PersonBirthLocation>
  <PersonPhysicalDetails>
    <PersonHeightMeasure personHeightUnitCode=”ncic”>602
        </PersonHeightMeasure>
    <PersonSexCode>M</PersonSexCode>
  </PersonPhysicalDetails>
  <PersonSocialDetails>
    <PersonCitizenshipCode.fips10-4>
       US</PersonCitizenshipCode.fips10-4>
  </PersonSocialDetails>
  <PersonBiometricDetails>
    <PersonFingerprintSet>
      <Fingerprint>
        <FingerprintFingerCode>3</FingerprintFingerCode>
        <FingerprintPatternCode>XX</FingerprintPatternCode>
      </Fingerprint>
    </PersonFingerprintSet>
  </PersonBiometricDetails>
  <Employment>
    <EmploymentEmployerName>RT</EmploymentEmployerName>
    <EmploymentLocation>
      <LocationAddress>
        <LocationStreet>
          <StreetFullText>1600 Pennsylvania Avenue NW
               </StreetFullText>
        </LocationStreet>
        <LocationCityName>Washington</LocationCityName>
        <LocationStateCode.USPostalService>DC
               </LocationStateCode.USPostalService>
        <LocationPostalCodeID>
```



```
                  <ID>20002</ID>
                </LocationPostalCodeID>
                <LocationCountryCode.fips10-4>US
                       </LocationCountryCode.fips10-4>
              </LocationAddress>
            </EmploymentLocation>
          </Employment>
        </Person>
        <DriverAuthorization>
          <DriverAuthorizationID.Detailed>
            <ID>TT12345222</ID>
            <IDJurisdictionCode.ncicLIS>DC
                     </IDJurisdictionCode.ncicLIS>
          </DriverAuthorizationID.Detailed>
        </DriverAuthorization>
        <RTDocument>
        <DocumentTitle>US_PASSPORT</DocumentTitle>
        <Document>
          <DocumentBinary>
            <BinaryObject.Base64>R0dkieDlhcgGSALMAA</BinaryObject.Base64>
          <DocumentBinary>
          <DocumentDescriptiveMetadata>
            <DocumentSequenceID>
              <ID>1</ID>
            </DocumentSequenceID>
            <DocumentTitleText>US Passport</DocumentTitleText>
            <DocumentDescriptionText>Captured using XYZ
                Scanner</DocumentDescriptionText>
            <DocumentDisputedReasonText>Damaged
                </DocumentDisputedReasonText>
          </DocumentDescriptiveMetadata>
        </Document>
        </RTDocument>
        <RTDocument>
        <DocumentTitle>STATE_ISSUED_DRIVER_LICENSE_OR_ID</DocumentTitle>
        <Document>
          <DocumentBinary>
            <BinaryObject.Base64>R0dkieDlhcgGSALMAA</BinaryObject.Base64>
          <DocumentBinary>
          <DocumentDescriptiveMetadata>
            <DocumentSequenceID>
              <ID>2</ID>
            </DocumentSequenceID>
            <DocumentTitleText>ID Card</DocumentTitleText>
          </DocumentDescriptiveMetadata>
        </Document>
        </RTDocument>
        <ImageCaptureDevice>
              <CaptureDeviceMakeText>DBI</CaptureDeviceMakeText>
              <CaptureDeviceModelText>1134</CaptureDeviceModelText>
              <CaptureDeviceSerialNumberText>12345</CaptureDeviceSerialNu
              mberText>
        </ImageCaptureDevice>
      </OtherDescriptiveText>
    </UserDefinedDescriptiveText>
  </ITLUserDefinedDescriptiveTextRecord>
```


Note that the first Image Designation Character in the enrollment message shall start at ‘00’ and that subsequent records shall be consecutively incremented.

4.3.8.2 Type-14: Variable-Resolution Fingerprint Image Record

The Type-14 records follow the proposed changes as stated by ANSI/NIST-ITL 1-2000 - XML Representation and the schema defined by http://www.doj.state.wi.us/les/NIST-ITL/index.htm.

The following shows an example of the Type-14 data:

```
<ITLVariableResolutionFingerprintImageRecord>
<ImageDesignationCharacter>01</ImageDesignationCharacter>
  <SourceAgency>
    <OrganizationName>EP</OrganizationName>
  </SourceAgency>
  <TenprintCaptureDate>2005-11-15</TenprintCaptureDate>
  <PersonFingerprint>
    <FingerImpressionTypeCode>0</FingerImpressionTypeCode>
    <FingerPosition>
      <FingerPositionCode>14</FingerPositionCode>
    </FingerPosition>
    <FingerprintSegmentationData>
      <SegmentationDetail>
        < FingerPositionCode>7</FingerPositionCode>
        <LeftXCoordinate>1123</LeftXCoordinate>
        <RightXCoordinate>1442</RightXCoordinate>
        <TopYCoordinate>371</TopYCoordinate>
        <BottomYCoordinate>871</BottomYCoordinate>
      </SegmentationDetail>
      <SegmentationDetail>
        <FingerPositionCode>8</FingerPositionCode>
        <LeftXCoordinate>776</LeftXCoordinate>
        <RightXCoordinate>1093</RightXCoordinate>
        <TopYCoordinate>47</TopYCoordinate>
        <BottomYCoordinate>589</BottomYCoordinate>
      </SegmentationDetail>
      <SegmentationDetail>
        <FingerPositionCode>9</FingerPositionCode>
        <LeftXCoordinate>432</LeftXCoordinate>
        <RightXCoordinate>770</RightXCoordinate>
        <TopYCoordinate>138</TopYCoordinate>
        <BottomYCoordinate>700</BottomYCoordinate>
      </SegmentationDetail>
      <SegmentationDetail>
        <FingerPositionCode>10</FingerPositionCode>
        <LeftXCoordinate>16</LeftXCoordinate>
        <RightXCoordinate>287</RightXCoordinate>
        <TopYCoordinate>642</TopYCoordinate>
        <BottomYCoordinate>1171</BottomYCoordinate>
      </SegmentationDetail>
    </FingerprintSegmentationData>
    <FingerprintNISTImageQualityData>
      <NISTImageQualityDetail>
        <FingerPositionCode>7</FingerPositionCode>
        <NISTImageQualityMeasure>4</NISTImageQualityMeasure>
      </NISTImageQualityDetail>
      <NISTImageQualityDetail>
```



```
            <FingerPositionCode>8</FingerPositionCode>
            <NISTImageQualityMeasure>1</NISTImageQualityMeasure>
          </NISTImageQualityDetail>
          <NISTImageQualityDetail>
            <FingerPositionCode>9</FingerPositionCode>
            <NISTImageQualityMeasure>1</NISTImageQualityMeasure>
          </NISTImageQualityDetail>
          <NISTImageQualityDetail>
            <FingerPositionCode>10</FingerPositionCode>
            <NISTImageQualityMeasure>2</NISTImageQualityMeasure>
          </NISTImageQualityDetail>
        </FingerprintNISTImageQualityData>
      </PersonFingerprint>
      <Image>
        <ImageHorizontalLineLength>1600</ImageHorizontalLineLength>
        <ImageVerticalLineLength>976</ImageVerticalLineLength>
        <ImageScaleUnitsCode>1</ImageScaleUnitsCode>
        <ImageHorizontalPixelScale>500</ImageHorizontalPixelScale>
        <ImageVerticalPixelScale>500</ImageVerticalPixelScale>
        <ImageCompressionAlgorithmText>WSQ
          </ImageCompressionAlgorithmText>
        <ImageBitsPerPixel>8</ImageBitsPerPixel>
        <ImageObject.Base64>base64+content</ImageObject.Base64>
      </Image>
    </ITLVariableResolutionFingerprintImageRecord>
```

Note that there should be three (3) such Type-14 records included in each enrollment request message (assuming no amputations that prohibit the capture of one of the three slap images).

4.3.8.3 Type-99: CBEFF Data Records

The Type-99 records, ITLCBEFFImageRecord, are used to exchange biometric data that conforms to INCITS 398-2005, the Common Biometric Exchange Formats Framework (CBEFF). A CBEFF compliant Biometric Information Record (BIR) used by the Type-99 logical record is based on a common Header and a Biometric Data Block (BDB).

The following two examples show Type-99, CBEFF Data Records, iris and face:

```
    <ITL-CBEFFBiometricDataRecord nist:typeCode="99">
      <ImageDesignationCharacter>05</ImageDesignationCharacter>
      <SourceAgency>
        <OrganizationName>EP</OrganizationName>
      </SourceAgency>
      <BiometricCaptureDate>2006-07-07</BiometricCaptureDate>
      <CBEFFHeaderVersionNumber>0101</CBEFFHeaderVersionNumber>
      <BiometricTypeCode>00000010</BiometricTypeCode>
      <BiometricQualityData>
        <QualityMeasure>100</QualityMeasure>
        <QualityAlgorithmVendorID>
          <ID>String</ID>
        </QualityAlgorithmVendorID>
        <QualityAlgorithmProductCodeNumber>01
              </QualityAlgorithmProductCodeNumber>
        <QualityAlgorithmVersionNumber>String
              </QualityAlgorithmVersionNumber>
      </BiometricQualityData>
      <CBEFFBiometricDataBlockFormatOwnerID>
```



```
      <ID>0101</ID>
    </CBEFFBiometricDataBlockFormatOwnerID>
    <CBEFFBiometricDataBlockFormatTypeID>
      <ID>0009</ID>
    </CBEFFBiometricDataBlockFormatTypeID>
    <UserDefinedFields>
      <SBHSecurityOptions>00</SBHSecurityOptions>
      <ValidityPeriod>0000000000000000</ValidityPeriod>
      <BiometricDataType>00100000</BiometricDataType>
      <FASCN>00000000000000000000000000</FASCN>
      <PatronHeaderVersion>03</PatronHeaderVersion>
    </UserDefinedFields>
    <CBEFFBinaryDataBlock.Base64>base64+content
          </CBEFFBinaryDataBlock.Base64>
  </ITL-CBEFFBiometricDataRecord >
```

Note that there will be 0, 1, or 2 such Type-99 iris records included in the enrollment message, depending on the number of iris images captured.

```
  <ITL-CBEFFBiometricDataRecord nist:typeCode="99">
    <ImageDesignationCharacter>07</ImageDesignationCharacter>
    <SourceAgency>
      <OrganizationName>EP</OrganizationName>
    </SourceAgency>
    <BiometricCaptureDate>2006-07-07</BiometricCaptureDate>
    <CBEFFHeaderVersionNumber>0101</CBEFFHeaderVersionNumber>
    <BiometricTypeCode>00000002</BiometricTypeCode>
    <BiometricQualityData>
      <QualityMeasure>-2</QualityMeasure>
      <QualityAlgorithmVendorID>
        <ID>String</ID>
      </QualityAlgorithmVendorID>
      <QualityAlgorithmProductCodeNumber>0
            </QualityAlgorithmProductCodeNumber>
      <QualityAlgorithmVersionNumber>String
            </QualityAlgorithmVersionNumber>
    </BiometricQualityData>
    <CBEFFBiometricDataBlockFormatOwnerID>
      <ID>001B</ID>
    </CBEFFBiometricDataBlockFormatOwnerID>
    <CBEFFBiometricDataBlockFormatTypeID>
      <ID>0501</ID>
    </CBEFFBiometricDataBlockFormatTypeID>
    <UserDefinedFields>
      <SBHSecurityOptions>00</SBHSecurityOptions>
      <ValidityPeriod>0000000000000000</ValidityPeriod>
      <BiometricDataType>00100000</BiometricDataType>
      <FASCN>00000000000000000000000000</FASCN>
      <PatronHeaderVersion>03</PatronHeaderVersion>
    </UserDefinedFields>
    <CBEFFBinaryDataBlock.Base64>base64+content
          </CBEFFBinaryDataBlock.Base64>
  </ITL-CBEFFBiometricDataRecord >
```


4.3.9 Status Code

The status code provides return values to the requesting system to inform of processing success or errors. The intent of the status code is to support automated interpretation of the requested operation; thus, values must be precisely as shown here (case significant). If further information is to be provided, an additional "reason" field (status message) is separately available. The final list of status codes will be in the published schema. The following values are presently defined for this field with more expected to be added as required:

- OK: request processed as expected.
- Unknown: an unknown error has occurred.
- EnrollmentDataFormatNotValid: the data provided is not of valid format for the type data specified.
- CertificateNotSignedByCIMS: the Private Information Key certificate specified is not signed by the CIMS. Only certificates signed by the CIMS are acceptable.
- CertificateNotValid: the validity period for the certificate specified is not current.
- FailureToGenerateCardPayload: the enrollment or re-issuance request was unable to generate a card payload from the RT Participant's data.
- IllFormedCertificate: the certificate specified is not of valid format.
- IllFormedPublicKey: the public key specified is not of valid format.
- IncompleteEnrollmentData: required data for an enrollment record was not included with the enrollment request.
- InvalidADSN: the message has an invalid ADSN. The ADSN specified has been revoked, does not exist, or does not match the RTID specified.
- InvalidQuality: the message does not meet minimum biometric quality requirements.
- InvalidRTID: the message has an invalid RTID. The RTID specified has been revoked, does not exist, or does not match the SPID specified.
- InvalidSPID: the message has an invalid SPID. The SPID specified has been revoked or does not exist.
- MalformedEnrollmentData: the enrollment record was not correctly sent.
- NonExistentContentType: the requested content type is not defined in the system.
- RequestXMLNotValid: the XML request is not valid.
- RequestXMLNotWellFormed: the XML request is not well formed.

The XML definition for this type is:

```
<xs:simpleType name="StatusCodeType">
  <xs:restriction base="xs:string">
    <xs:enumeration value="OK"/>
    <xs:enumeration value="Unknown"/>
    <xs:enumeration value="EnrollmentDataFormatNotValid"/>
    <xs:enumeration value="CertificateNotSignedByCIMS"/>
    <xs:enumeration value="CertificateNotValid"/>
```



```
        <xs:enumeration value="FailureToGenerateCardPayload"/>
        <xs:enumeration value="IllFormedCertificate"/>
        <xs:enumeration value="IllFormedPublicKey"/>
        <xs:enumeration value="InvalidADSN"/>
        <xs:enumeration value="InvalidQuality"/>
        <xs:enumeration value="InvalidRTID"/>
        <xs:enumeration value="InvalidSPID"/>
        <xs:enumeration value="IncompleteEnrollmentData"/>
        <xs:enumeration value="MalformedEnrollmentData"/>
        <xs:enumeration value="NonExistentContentType"/>
        <xs:enumeration value="RequestXMLNotValid"/>
        <xs:enumeration value="RequestXMLNotWellFormed"/>
      </xs:restriction>
    </xs:simpleType>
```

The following example shows a sample status message:

```
<Status>OK</Status>
```

4.3.10 Payload Acknowledgement Type

The payload acknowledgement message is used to acknowledge that the card payload has been successfully received from the CIMS. Once the acknowledgement message has been received from the EP, the CIMS can remove the biographic data.

The schema definition for this message content consists of the following elements:

```
<xs:complexType name="PayloadAcknowledgementType">
  <xs:sequence>
    <xs:element name="StatusCode" type="StatusCodeType"/>
  </xs:sequence>
</xs:complexType>
```

The following example shows a sample payload acknowledgement message:

```
<EPCHEnrollmentConfirmation>
  <StatusCode>OK</StatusCode>
<EPCHEnrollmentConfirmation>
```

4.3.11 Requested Fingers

The Requested Fingers object provides the preferred inclusion of biometrics for template creation. Because all fingerprints will not be on the card, it is important that the RT Applicant's preferred fingerprints be known when creating the templates. The CIMS will use the requested biometrics if the quality score is achieved and a template can be created.

The schema definition for requested biometrics:

```
<xs:simpleType name="RequestedFingersType">
  <xs:restriction base="xsd:string">
    <xs:pattern value="\d+,\d+,\d+,\d+"/>
  </xs:restriction>
</xs:simpleType>
```

The following values are presently defined for this field as specified using ANSI/NIST ITL 1-2006 Table 12:

Finger Position	Value
No selection	0

Right thumb	1
Right index	2
Right middle	3
Right ring	4
Right little	5
Left thumb	6
Left index	7
Left middle	8
Left ring	9
Left little	10

Table 4-1. Requested Finger Position Codes

The following example shows requested fingers:

```
<RequestedFingers>2,3,6,7</RequestedFingers>
```

NOTE: If the event of an enrollment exception (i.e., waiver for 2 good fingers rather than 4), the RequestedFingers line above would appear as follows:

```
<RequestedFingers>2,7,0,0</RequestedFingers>
```

4.3.12 Processing Group

The Processing Group object identifies the group to which the subject of the enrollment request belongs, identifying them as officers, enrollment officers, travelers, and pilot participants. This information will assist TSA in making adjudication decisions.

The following values are presently defined for this field:

- RTPART: Registered Traveler Participant
- SPOFFICER: Service Provider Officer
- SPEMPLOYEE: Service Provider Employee
- RTPILT: Registered Traveler Participant that have been pre-approved by the TSA for submittal without the initial RT fee

Note: Future additions to the ProcessingGroup element will be handled by the TSA and CIMS without the requirement for the RTIC to evaluate additional values.

The schema definition for ProcessingGroup is:

```
<xs:simpleType name="ProcessingGroupType">
   <xs:restriction base="xs:string">
      <xs:enumeration value="RTPART”/>
      <xs:enumeration value="SPOFFICER”/>
      <xs:enumeration value="SPEMPLOYEE"/>
      <xs:enumeration value="RTPILT"/>
   </xs:restriction>
</xs:simpleType>
```

4.4 RT Applicant Enrollment and Card Issuance

RT Applicant enrollment and card issuance are used to provide an RT Applicant's enrollment data for a Security Threat Assessment, to create the card payload, and to issue a card to an approved RT Participant. The following flow diagram shows the processing stages that are performed during RT Applicant enrollment and card issuance:

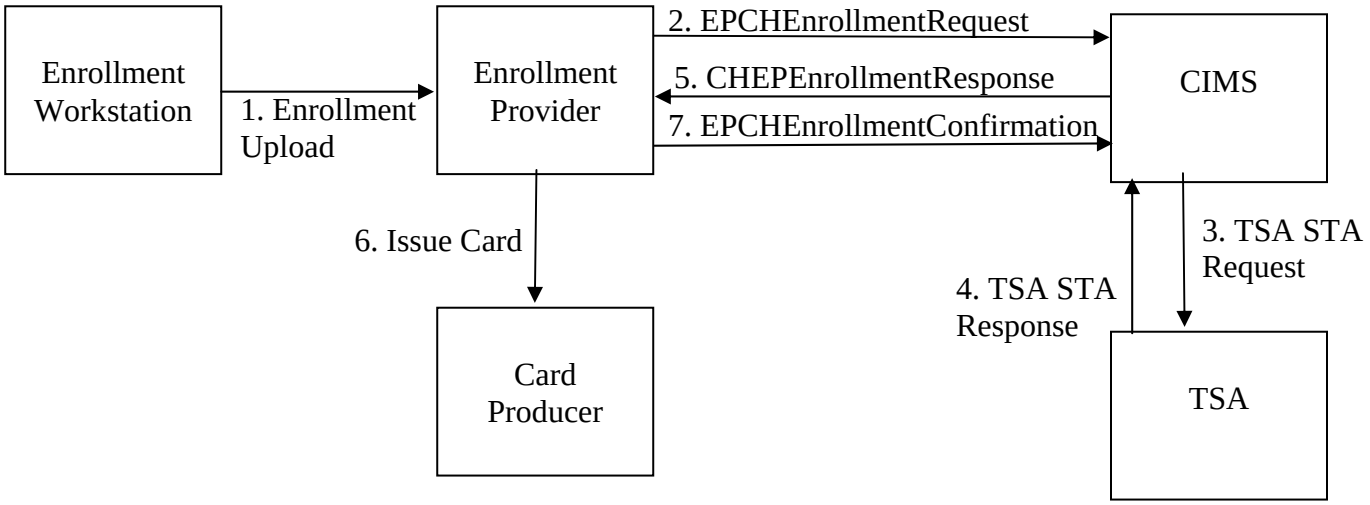


Figure 4-1. Traveler Enrollment and Card Issuance

4.4.1 Enrollment Upload

The enrollment capture and upload processing is performed by the EP to transmit the data to a central EP center. Because this describes a processing step, no contents are described.

4.4.2 EPCH Enrollment Request

This encrypted message is sent from an EP to the CIMS to enroll an RT Applicant in the RT program, perform an RT Applicant STA, and obtain the authentication payload for a new card.

```
<Content>
  <EncryptedData Id="DOC" xmlns="http://www.w3.org/2001/04/xmlenc#"
           Type="http://www.w3.org/2001/04/xmlenc#Content">
    <EncryptionMethod
           Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:RetrievalMethod URI="#KEY"
           Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey"/>
      <ds:KeyName>TemporaryKey</ds:KeyName>
    </ds:KeyInfo>
    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <EncryptedKey Id="KEY" xmlns="http://www.w3.org/2001/04/xmlenc#">
        <EncryptionMethod
             Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
        <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
          <ds:KeyName>ProviderKey</ds:KeyName>
        </ds:KeyInfo>
```



```
            <CipherData>
              <CipherValue>encrypted+key</CipherValue>
            </CipherData>
            <ReferenceList><DataReference URI=”#DOC”/></ReferenceList>
            <CarriedKeyName>TemporaryKey</CarriedKeyName>
          </EncryptedKey>
        </ds:KeyInfo>
        <CipherData>
           <CipherValue>base64+encrypted+content</CipherValue>
        </CipherData>
      </EncryptedData>
    </Content>
```

Where the encrypted data content after decryption would contain the following:

```
<EPCHEnrollmentRequest>
  <RTID>A1B2C3D4E5F6G7H8</RTID>
  <EnrollmentOfficerID>john</EnrollmentOfficerID>
  <RequestedFingers>2,3,6,7</RequestedFingers>
  <EnrollmentData>[example suppressed due to length]</EnrollmentData>
</EPCHEnrollmentRequest>
```

The schema definition for this message content consists of the following elements:

```
<xs:element name="EPCHEnrollmentRequest" type="EnrollmentRequestType"/>
<xs:complexType name="EnrollmentRequestType">
  <xs:sequence>
    <xs:element name="RTID" type="IdentifierType" />
    <xs:element name="EnrollmentOfficerID" type="xs:string" />
    <xs:element name=”SponsoringEntity” type=”SponsoringEntityType” />
    <xs:element name="RequestedFingers" type="RequestedFingersType”
                minOccurs="0" />
    <xs:element name="Resubmit" type="ResubmitType" minOccurs="0" />
    <xs:element name=”EnrollmentException”
Type=”EnrollmentExceptionType” minOccurs="0" />
   <xs:element name="EnrollmentData" type="NIST-
ITLBiometricInformationExchangePackageType" />
  </xs:sequence>
</xs:complexType>
```

<RTID> provides the RT Applicant’s identifier as determined by the SP. This identifier is assigned when the RT Applicant is first enrolled by the EP and remains unchanged throughout the association of the RT Applicant and the SP. This value allows the CIMS to determine the specific RT Applicant’s record being referenced. See the description of an identifier in Section 4.3.2, Identifier.

<EnrollmentOfficerID> specifies the SP’s identifier for the Enrollment Officer that performed the enrollment.

<SponsoringEntity> specifies the sponsoring entity with which the enrollment is associated (e.g., the airport at which the enrollment occurred and/or by which the enrolling SP is sponsored). The content will normally be an airport or airline code.

The schema definition for SponsoringEntityType is:

```
<xs:simpleType name="SponsoringEntityType">
      <xs:restriction base="xs:string">
            <xs:length value="4"/>
```



```
            </xs:restriction>
      </xs:simpleType>
```

<RequestedFingers> provides the desired fingers which the RT Applicant would prefer to use for verification (or which the EP is selecting for the RT Applicant). CIMS may not be able to support the requested fingers if it fails to generate the requested templates. The EP must check the payload record to determine the actual fingers that are available.

<Resubmit> defines the type of enrollment submission for an RT Applicant.

The schema definition for ResubmitType is:

```
      <xs:simpleType name="ResubmitType">
          <xs:restriction base="xs:string">
            <xs:enumeration value="NEW">
            <xs:enumeration value="RESUBMIT">
            <xs:enumeration value="REENROLL">
          </xs:restriction>
      </xs:simpleType>
```

where:

NEW is an initial submission which contains a full complement of enrollment data and for which full enrollment processing is performed.

RESUBMIT is performed on an ‘as required’ basis whenever applicant data has changed (e.g., name change due to marriage). In this case, the new data is provided, the CIMS database is updated, and TSA is notified, but no new payload is generated or card re-issued.

REENROLL uses the same SPID/RTID as originally assigned. A full set of new data is provided and the same process as NEW is followed except that a) a hit is expected during de-duplication (matching the original RTID) and b) the enrollment response does not wait for the STA response to be received (if the STA result is negative, a subsequent revocation will be issued.)

<EnrollmentException> is a flag which identifies an individual as being exempt from the requirement to provide at least 4 fingerprints meeting minimum quality requirements. (These individuals must still provide at least 2 fingerprints meeting these requirements.)

The schema definition for EnrollmentExceptionType is:

```
      <xs:simpleType name="EnrollmentExceptionType">
            <xs:restriction base="xs:string">
                  <xs:enumeration value="WAIVER"/>
            </xs:restriction>
      </xs:simpleType>
```

<EnrollmentData> provides the enrollment data from the SP. This data format is specified in Section 4.3.8, EnrollmentData.

4.4.3 TSA STA Request

This step denotes the CIMS sending data to the TSA to perform a STA for an RT Applicant. The content of the message will be defined by the TSA and the CIMS.

4.4.4 TSA STA Response

This step denotes the TSA sending a response to the CIMS for the STA. The content of the message will be defined by the TSA and the CIMS.

4.4.5 CHEP Enrollment Response

```
<Content>
  <EncryptedData Id=”DOC” xmlns=”http://www.w3.org/2001/04/xmlenc#”
          Type=”http://www.w3.org/2001/04/xmlenc#Content”>
    <EncryptionMethod
          Algorithm=”http://www.w3.org/2001/04/xmlenc#aes256-cbc”/>
    <ds:KeyInfo xmlns:ds=”http://www.w3.org/2000/09/xmldsig#”>
      <ds:RetrievalMethod URI=”#KEY”
          Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey"/>
      <ds:KeyName>TemporaryKey</ds:KeyName>
    </ds:KeyInfo>
    <ds:KeyInfo xmlns:ds=”http://www.w3.org/2000/09/xmldsig#”>
      <EncryptedKey Id=”KEY” xmlns=”http://www.w3.org/2001/04/xmlenc#”>
        <EncryptionMethod
            Algorithm=”http://www.w3.org/2001/04/xmlenc#rsa-1_5”/>
        <ds:KeyInfo xmlns:ds=”http://www.w3.org/2000/09/xmldsig#”>
          <ds:KeyName>ProviderKey</ds:KeyName>
        </ds:KeyInfo>
        <CipherData>
          <CipherValue>encrypted+key</CipherValue>
        </CipherData>
        <ReferenceList><DataReference URI=”#DOC”/></ReferenceList>
        <CarriedKeyName>TemporaryKey</CarriedKeyName>
      </EncryptedKey>
    </ds:KeyInfo>
    <CipherData>
       <CipherValue>base64+encrypted+content</CipherValue>
    </CipherData>
  </EncryptedData>
</Content>
```

Where the encrypted data content after decryption would contain the following:

```
<CHEPEnrollmentResponse>
  <RTID>A1B2C3D4E5F6G7H8</RTID>
  <TSAReferenceNumber>TSA123456789</TSAReferenceNumber>
  <ADSN>3</ADSN>
  <Expire>2010-06-28</Expire>
  <Payload>
    <FingerprintObjectOne>base64+content</FingerprintObjectOne>
    <FingerprintObjectTwo>base64+content</FingerprintObjectTwo>
    <IrisObject>base64+content</IrisObject>
    <FacialObject>base64+content</FacialObject>
    <PersonalDataObject>base64+content</PersonalDataObject>
    <SecurityDataAuthObject>base64+content</SecurityDataAuthObject>
    <CardKey>base64+content</CardKey>
    <KeyVersion>1</KeyVersion>
  </Payload>
  <StatusCode>OK</StatusCode>
</CHEPEnrollmentResponse>
```

This shows the response returned by the CIMS to the EP for STA information, Card Payloads, and Card Issuance Information. The response message provides the status of the enrollment and card issuance request.

The schema definition for this message content consists of the following elements:

```
<xs:element name="CHEPEnrollmentResponse"
type="EnrollmentResponseType"/>

<xs:complexType name="EnrollmentResponseType">
  <xs:sequence>
    <xs:element name="RTID" type="IdentifierType" />
    <xs:element name="TSAReferenceNumber" type="xs:string"
                minOccurs="0" />
    <xs:element name="ADSN" type="ADSNType" minOccurs="0" />
    <xs:element name="Expire" type="xs:date" minOccurs="0" />
    <xs:element name="Payload" type="AuthPayloadType" minOccurs="0" />
    <xs:element name="StatusCode" type="StatusCodeType" />
    <xs:element name="StatusMessage" type="xs:string" minOccurs="0" />
  </xs:sequence>
</xs:complexType>
```

<RTID> provides the RT Applicant's identifier as determined by the SP. This identifier is assigned when the RT Applicant is first enrolled by this EP and remains unchanged throughout the association of the RT Applicant and the SP. This value allows the CIMS to determine the specific RT Applicant's record being referenced. See the description of an identifier in Section 4.3.2, Identifier.

<TSAReferenceNumber> provides the TSA Reference Number used as TSA Case Number. This value is typically used by the RT Applicant if they wish to contact the TSA about a failed STA. This field may be empty if no case number was provided by the TSA.

<ADSN> specifies the current authentication data sequence number for this RT Applicant. In the reply message, Section 4.3.4, ADSN (Authentication Data Sequence Number), the CIMS will return the updated ADSN that is to be assigned to the newly issued card. This value is specified as a single alphanumeric character.

<Expire> provides the expiration date for the new card as managed by the CIMS. This value can be retained by the SP to record the card expiration date which may be different from the RT Participant's enrollment period with the EP. When this date is reached, the CIMS will automatically expire the card; a new card must be issued prior to this date to remain active. This value is a date string specifying century, year, month, and day of expiration.

<Payload> specifies the various elements that must be placed on the RT Participant's card. This is further broken into child elements to allow easier interaction between the EP and the card issuer. The EP must ensure these data elements are placed on the card without modification. The EP must also build and sign the card identifier field which is constructed of various ID fields.

<StatusCode> provides status codes for the interactions between SPs and the CIMS.

<StatusMessage> provides an optional human readable message related to the StatusCode.

4.4.6 Issue Card

This step denotes the EP sending the payload data to the card issuer. Since EPs might not themselves actually produce the cards, this step attempts to recognize this level of separation. The actual content of any message and format thereof is determined by the SP. Multiple interchanges are allowed and the EP may batch a series of card productions into a single request/response cycle. How the message is transferred is also at the determination of the SP although all RT level security requirements, Section 6, System Security, must be satisfied.

While the actual content of the message can be defined by the SP, there are specific data items returned by the CIMS that must be transferred to be placed on the card. These items are the RTID, ADSN, Expire and the Payload fields as described previously. The EP must also generate a digital signature that can be used to authenticate that the EP created the various fields.

4.4.7 EPCH Enrollment Confirmation

The payload acknowledgement is returned by the EP to CIMS to signify that the card payload has been successfully received and that the CIMS can delete the biographic data.

The XML schema for a verification notification is:

```
<xs:element name="EPCHEnrollmentConfirmation"
type="PayloadAcknowledgementType" />
```

The following example shows an example verification notification.

```
<EPCHEnrollmentConfirmation>
  <StatusCode>OK<StatusCode>
</EPCHEnrollmentConfirmation>
```

4.5 RT Participant Verification

Once an RT Participant has received their RT card, they are authorized to proceed through the RT lanes at all RT equipped airports they visit. Due to the variety of airport configurations, it may not be possible for all verification stations to support continual on-line activity. For this reason, the verification stage is considered to be a stand-alone activity. Yet to support financial activity auditing of verification events, it is necessary for the verification stations to record a certain level of information. How this information is then transferred from the verification station back to the VP's facility, and the format used, is not specified. The XML schema listed here is to denote the form by which the verification event set should be made available to the EP. Only the verification events for RT Participants registered with a specific EP should be submitted to that EP. When and at what frequency this data is passed to each EP is determined by the business arrangement between the individual verification and EPs. Events that occur against TSA-revoked cards are also submitted to CIMS independent of the card's EP (see below.)

The content specified here is the minimal level of information that should be obtained. This level of information is believed to be usable by the receiving EP to validate verification events without identifying the RT Participant as well as to determine usability events that could support general biometric usability trends.

Business policy prevents the VP from recording specific RT Participant identifying data such as the RTID or name. This VID is reported as the tracking identifier for each verification event. The TSA has required a deviation from this policy only when a card which has been TSA-revoked is used. In these events, the RTID shall be recorded and the verification event forwarded for TSA notification. The participant would

still be prevented from using their card as it is invalid (revoked), the only addition is the recording of the CardID (RTID+ADSN; see TSAEvent in Section 4.5.3, VPCH Verification Event). When the VP uploads this event, they must also separate such verification events and forward these to the CIMS for TSA notification. It is required that a VP upload any such event within 24 hours of it occuring. The CIMS shall notify the TSA within 12 hours of it receiving the event from the VP.

4.5.1 Verification Upload

Periodically the VP must transfer the verification event information that has been collected at the individual verification stations to their service facility. It is from the VP facility that all other operations with the data including distribution to other SPs are shown. The information listed below must be collected and retained for reporting.

4.5.2 VPEP Verification Event

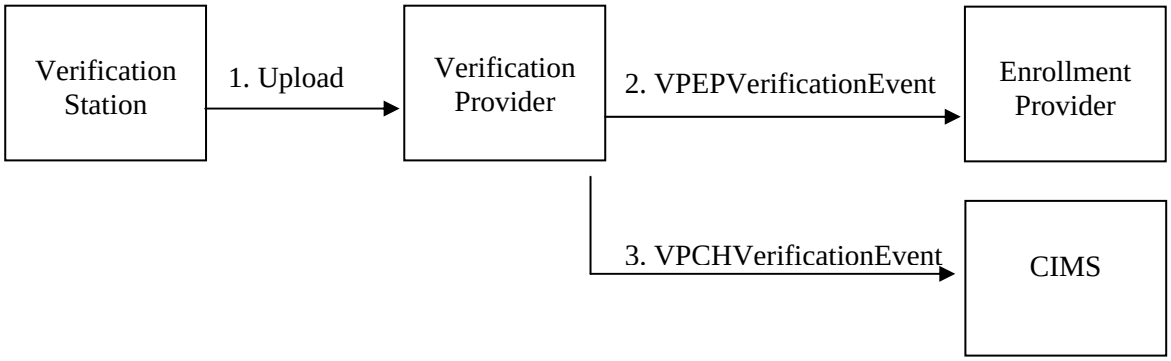


Figure 4-1. Verification of Traveler

The verification notification is passed from a VP to an EP to identify the events which have occurred. This message defines the series of events which occurred to constitute a verification activity for an RT Participant. Multiple verification activities may be combined into a single message when transmitting to an EP. When a VP processes an event with the TSAEvent field (see Section 4.5.3, VPCH Verification Event), they must also pass this event to CIMS for TSA notification.

The XML schema for a verification notification is shown below:

```
<xs:complexType name=”VPEPVerificationEvent”
type="VerificationEventsType" />

<xs:complexType name="VerificationEventsType">
  <xs:sequence>
    <xs:element name="Verification" type="VerificationEventType"
                maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="VerificationEventType">
  <xs:complexContent>
    <xs:extension base="VerificationCommonEventType">
      <xs:sequence>
        <xs:element name="VID" type="IdentifierType"/>
      </xs:sequence>
```



```
    </xs:extension>
  </xs:complexContent>
</xs:complexType>

<xs:complexType name="VerificationCommonEventType">
  <xs:sequence>
    <xs:element name="SPID" type="SPIDType"/>
    <xs:element name="StartAt" type="xs:dateTime"/>
    <xs:element name="EndAt" type="xs:dateTime"/>
    <xs:element name="AirportCode">
      <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:length value="3"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
    <xs:element name="Status" type="VerifyStatusType"/>
    <xs:element name="Reason" type="xs:string" minOccurs="0"/>
    <xs:element name="VerifyEvent" type="VerifyEventType" minOccurs="0"
                maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name=”VerifyEventType”>
  <xs:sequence>
    <xs:element name=”Timestamp” type=”xs:dateTime”/>
    <xs:element name=”Biometric” type=”xs:int” maxOccurs="unbounded" />
    <xs:element name=”Quality” type=”xs:int”/>
    <xs:element name=”Status” type=”VerifyStatusType”/>
    <xs:element name=”Reason” type=”xs:string” minOccurs=”0”/>
  </xs:sequence>
</xs:complexType>

<xs:simpleType name=”VerifyStatusType”>
  <xs:restriction base=”xs:string”>
    <xs:length value=”4”/>
    <xs:enumeration value=”PASS”/>
    <xs:enumeration value=”FAIL”/>
  </xs:restriction>
</xs:simpleType>
```

<Verification> This provides a list of one or more verification events that occurred and the time at which each occurred. The values which are constant to the verification event are provided here and each event then follows. A single verification record should be used for each verification attempt consisting of one or more events. Multiple verifications are allowed to be specified in a single message in sending to the EP but only those events for RT Participants belonging to the EP should be included.

<SPID> The RT Participant’s EP obtained from the card is listed. Note this is the provider ID from the card, not the verification provider ID which would be specified in the header. This value would also denote the destination of this message.

<VID> The verification ID (VID) read from the RT Participant’s card is provided to identify which card was presented to the verification station.

<StartAt> The starting date/time when the card was presented and read by the verification station is recorded. This will allow computation of the time required for each verification event itself. This should be the full date/time to a minimum resolution of one second.

<EndAt> The completion date/time of all verification events for this RT Participant, typically the time at which the card was removed from the verification station. This allows computation of an overall elapsed time to verify this RT Participant.

<AirportCode> The standard IATA 3-letter airport code should be provided as a means of identifying the airport at which the verification event occurred. Specifying the particular verification station is not desired to avoid the ability to record specific traveler movement.

<Status> The final verification status, either PASS or FAIL, is given. Notice that each verification event also contains a status. The status field is meant to be machine readable, thus, only status types PASS or FAIL shall be used.

<Reason> This optional field is available to return more information about the reason for failure. The contents here might specify “unreadable card,” “expired card,” or “revoked card,” or any of a variety of other values. This field is simple text; no specification on the contents has been given. VPs are encouraged to make this information as meaningful as possible particularly for verification failures. If the status is PASS, this field becomes less important and may be dropped.

<VerifyEvent> This provides information on a specific verification event as more than one may be required to validate the RT Participant. This subfield may not exist if no biometric verification events were processed; potentially due to an invalid card or card read errors.

<Timestamp> The date/time at which the verification event (biometric capture/match) occurred. The difference between this timestamp and any prior or following timestamp provides a general estimate of how long the event itself required.

<Biometric> Identifies the biometric that was attempted for verification using the codes as specified in Section 5.3.7, Personal Data Object. If the event did not reference a biometric, the value of this field can be specified as zero (0). Multiple biometric fields should be used if multiple biometrics were involved in the verification; perhaps if multi-finger fusion is used.

<Quality> Provides the measured quality value of the biometric, either NFIQ for fingerprint, or iris quality Section 3, Biometric Data Management and Use. This can be used by the EP to determine general trends in quality of various biometrics. If the event did not reference a biometric, this value can be specified as zero (0). Multiple quality values may occur if multiple biometrics were considered.

<Status> Provides status of this specific verification event, either PASS or FAIL. Only the last event should contain PASS unless the overall verification failed. This field is meant to be machine readable thus only the two words PASS or FAIL shall be used.

<Reason> This optional field is available to return more information about the cause of event failure. This field is simple text, no specification on the content has been given. VPs are encouraged to make this information as meaningful as possible particularly for verification failures. If the status is PASS, this field may be dropped.

The following example shows an example verification notification:

```
<VPEPVerificationEvent>
  <Verification>
    <SPID>AA</SPID>
```



```
      <StartAt>2000-03-04T20:00:00Z </StartAt>
      <EndAt>2000-03-04T20:02:00Z </EndAt>
      <AirportCode>IAD</AirportCode>
      <Status>PASS</Status>
      <Reason>Biometric match</Reason>
      <VerifyEvent>
        <Timestamp>2000-03-04T20:00:00Z</Timestamp>
        <Biometric>9</Biometric>
        <Quality>4</Quality>
        <Status>FAIL</Status>
        <Reason>Capture quality too low</Reason>
      </VerifyEvent>
      <VerifyEvent>
        <Timestamp>2000-03-04T20:01:00Z</Timestamp>
        <Biometric>9</Biometric>
        <Quality>1</Quality>
        <Status>FAIL</Status>
        <Reason>Non-match</Reason>
      </VerifyEvent>
      <VerifyEvent>
        <Timestamp>2000-03-04T20:02:00Z</Timestamp>
        <Biometric>1</Biometric>
        <Quality>83</Quality>
        <Status>PASS</Status>
      </VerifyEvent>
      <VID>A1B2C3D4E5F6G7H8</VID>
    </Verification>
  </VPEPVerificationEvent>
```

4.5.3 VPCH Verification Event

When a verification event occurs that causes addition of the TSAEvent field due to attempted use of a TSA-revoked or suspended card, the VP must also forward this event to the CIMS. The CIMS will in turn notify the TSA of the condition. TSA events are the only ones that contain the RT Participant identifiers including the Card ID (SPID+RTID+ADSN).

```
<xs:element name="VPCHVerificationEvent"
type="TSAVerificationEventsType"/>
<xs:complexType name="TSAVerificationEventsType">
  <xs:sequence>
    <xs:element name="Verification" type="TSAVerificationEventType"
                maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>
<xs:complexType name="TSAVerificationEventType">
  <xs:complexContent>
    <xs:extension base="VerificationCommonEventType">
      <xs:sequence>
        <xs:element name="TSAEvent" type="TSAEventDetailsType" />
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>
<xs:complexType name="TSAEventDetailsType">
  <xs:attribute name="rtid" type="IdentifierType"/>
  <xs:attribute name="adsn" type="ADSNType"/>
```



```
    <xs:attribute name="state" type="RevokeActionType"/>
    <xs:attribute name="station" type="xs:string"/>
  </xs:complexType>
```

<TSAEvent> This field is used when a verification attempt against a TSA revoked or suspended card is attempted. When the Card ID (SPID+RTID+ADSN) or RT Participant (SPID+RTID) is located on the CRL and the action is a TSA event, the VP must also record this information for TSA notification. This tag consists of four required attributes, “RTID”, “ADSN”, “State”, and “Station”. The first two are used to specify the traveler and card, the third specifies the state of the card, and the fourth provides a specific verification station ID as defined by the VP. The field itself may optionally contain additional text that the VP believes is of benefit. This field is the only allowable means by which the traveler’s identity is recorded during verification and can only be used for TSA-related card states.

In the example below, a TSA_REVOKED_RTP card was presented for verification at the verification station termed “Gate72.” The status is FAIL because the card was invalid, the additional information is also specified to identify the specific card:

```
<VPCHVerificationEvent>
  <Verification>
    <SPID>AA</SPID>
    <StartAt>2000-03-04T20:00:00Z </StartAt>
    <EndAt>2000-03-04T20:00:10Z </EndAt>
    <AirportCode>IAD</AirportCode>
    <Status>FAIL</Status>
    <TSAEvent rtid=”12345-ABCDE-0000” adsn=”2”
              state=”TSA_REVOKED_RTP” station=”Gate72” />
  </Verification>
</VPCHVerificationEvent>
```

4.6 RT Participant Revocation

The TSA performs a continual STA on each RT Participant registered in the program and can at any time revoke an RT Participant’s participation in the program. Similarly an RT Participant may decide they no longer want to participate and may resign from their EP. Closing activity with one EP does not imply that they resign from the program overall. It is fully recognized that over time RT Participants may change SPs either by allowing their membership to lapse or canceling membership. Finally RT Participant cards can be lost or stolen and must be revoked to prevent unauthorized use thereof.

This activity covers both revocation (typically this is permanent) and suspension (which is temporary). Suspension might be used to temporarily prevent RT privileges while an issue of concern with the traveler is being resolved. Suspension also requires the ability to restore such privileges. All three types of conditions are performed: revoke, suspend, and restore.

Note that these messages document only the revocation action and not the distribution of the CRL. The provision of the revocation information to prevent use at verification is provided by Section 4.7, Card Revocation List Propagation, which occurs independently of this action.

4.6.1 Revocation Request and Response

While a revocation can originate from either the TSA or the EP use the same message type. The revocation action type provides the source of the revocation. When originating from the TSA, the CIMS

will forward a message to the EP. When originating from the EP, the CIMS will forward a message to the TSA if the revocation results in termination of the RT Participant from the RT program.

The XML schema for the revocation event is:

```
<xs:complexType name=”RevocationType”>
  <xs:sequence>
    <xs:element name=”RTID” type=”IdentifierType”/>
    <xs:element name=”ADSN” type=”ADSNType” minOccurs=”0”/>
    <xs:element name=”Action” type=”RevokeActionType”/>
    <xs:element name=”Cause” type=”xs:string” minOccurs=”0”/>
    <xs:element name="StatusCode" type="StatusCodeType" />
    <xs:element name="StatusMessage" type="xs:string" minOccurs="0"/>
  </xs:sequence>
</xs:complexType>
```

<RTID> The EP-unique RT Participant identifier that is being referenced. This value, along with the SPID in the message header, identifies the RT Participant for the CIMS to locate the record. On a revocation, the EP should recognize that no cards issued to this RT Participant will be accepted at a verification station.

<ADSN> The specific card sequence number being addressed. If the TSA revokes an RT Participant, this field is not used as all cards are by implication revoked. An EP may designate a specific card to revoke only that card or may leave this field off to revoke at the RT Participant level based on the action field.

<Action> Provides a machine readable value that denotes the revocation. For TSA revocations, this field will typically be “TSA_REVOKED_RTP” but other TSA actions are listed. The EP should specify the appropriate action based on the event that is causing the revocation. Note that the ADSN is required if only a single card is to be revoked.

When the revocation information is returned as part of the response, the action should be echoed back as a sign of success or returned as the value “NONE” to denote the action was not performed. If a cause is supplied on the response, it may contain more information. Revocation failures are not an automated process. Instead the EP is expected to contact CIMS and together they will resolve the problem.

<Cause> An optional string allowing a human readable explanation of the revocation. EP are encouraged to supply further information about the revocation event. This supports the TSA’s request to allow a designation as to why a revocation was performed and for TSA revocations may be the cause value on the permanent revocation entry. If this field is not supplied, the cause of revocation is unknown.

When supplied with a revocation response, this string should provide any additional details about the cause of the failure to perform the requested action.

<StatusCode> provides status codes for the interactions between SPs and the CIMS.

<StatusMessage> provides an optional human readable message related to the StatusCode.

4.6.2 Revocation of RT Participant by TSA

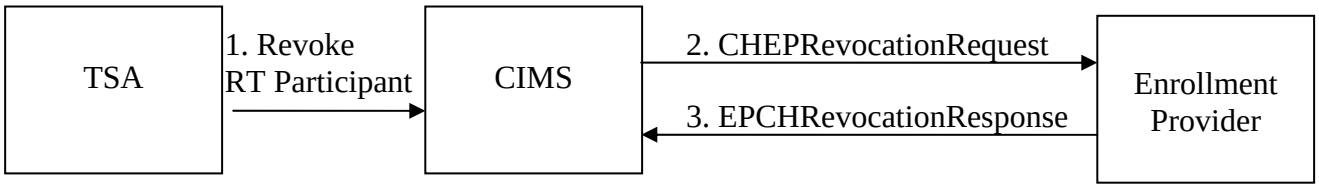


Figure 4-2. TSA Revocation of RT Participant

When the TSA determines that a specific RT Participant is no longer allowed privileges of the RT Program, they will request that all cards for that RT Participant be revoked. This request must be rapidly transmitted to the verification stations to prevent unauthorized use of RT privileges. This notice must also be passed to all EPs with whom the RT Participant is registered, notifying them of their member's revocation status.

4.6.2.1 The TSA Revokes an RT Participant

The TSA will notify the CIMS that a particular RT Participant's privileges should be immediately revoked. This will be done by providing the CIMS with the GUPID. The CIMS will then translate this into an RT Participant revocation for all SPs that have an RT Participant enrolled with the CIMS. The CIMS will then

send an updated CRL to all VPs to ensure that the cards involved are no longer authorized. The communication between the TSA and the CIMS is not specified here.

4.6.2.2 CHEP Revocation Request

In addition to adding the RT Participant to the permanent revocation list, the CIMS must also notify all EPs with whom the RT Participant is enrolled. The EPs in turn have the responsibility to notify their member and to update their records accordingly. This message is sent by the CIMS to each EP for which the RT Participant is enrolled using their RTID. The schema for this message is shown below:

```
<xs:element name="CHEPRevocationRequest" type="RevocationType"/>
```

See above for definition of the fields within the request message.

The following example shows a request revocation:

```
<CHEPRevocationRequest>
  <RTID>123-ABCD-45-6789</RTID>
  <Action>TSA_REVOKED_RTP</Action>
  <Cause>TSA request</Cause>
</CHEPRevocationRequest>
```

4.6.2.3 EPCH Revocation Response

This message acts as a confirmation by the EP that the requested RT Participant was identified and the revocation completed. The EP either echoes back the original action as a success or returns an action of NONE and optionally provides a status denoting a cause of failure. It is anticipated that manual intervention will be required if the action fails.

In the two examples shown here, the first is a successful TSA revocation, the second fails as the given RTID is unknown to this SP. The CIMS will not wait for the response before placing a revoked RT Participant on the revocation list for propagation to VPs. The schema is shown below:

```
<xs:element name="EPCHRevocationResponse" type="RevocationType"/>
```

See above for definition of the fields within the response message.

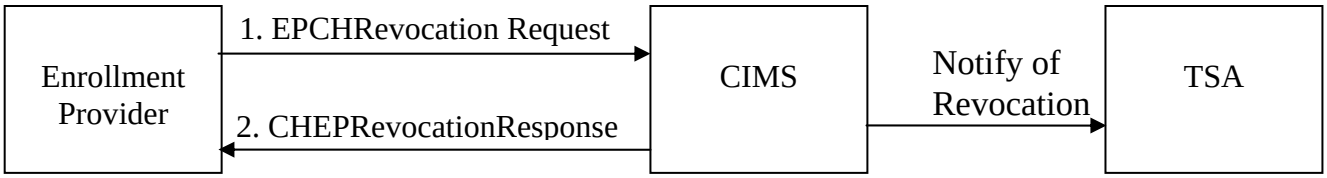
The following example shows a revocation response:

```
<EPCHRevocationResponse>
  <RTID>123-ABCD-45-6789</RTID>
  <Action>TSA_REVOKED_RTP</Action>
</EPCHRevocationResponse>

<EPCHRevocationResponse>
  <RTID>A1B2C3D4E5F6G7H8</RTID>
  <Action>NONE</Action>
  <Cause>No such RT Participant</Cause>
</EPCHRevocationResponse>
```

4.6.3 Revocation of Card or RT Participant by Enrollment Provider

When a card is lost or stolen, the RT Participant is expected to notify their EP and (typically) request a replacement card. The previous card needs to be marked as revoked to prevent unauthorized use. If the RT Participant resigns membership with a particular EP, all cards issued by that EP for that RT



Participant are revoked.

Figure 4-4. Provider Revocation of Card or RT Participant

4.6.3.1 EPCH Revocation Request

When an EP has to replace a member's card, or if the member decides not to renew their account, existing cards must be revoked so they cannot be used at the verification stations. This message allows the EP to notify the CIMS who will in turn add the card (or cards) to the revocation list and notify the TSA if revocation results in termination of participation in the RT program. The EP is encouraged to supply a more descriptive reason (cause) for the revocation to assist the TSA in tracking these events.

The XML schema for this message is shown below:

```
<xs:element name="EPCHRevocationRequest" type="RevocationType"/>
```

See above for an explanation of the revocation request fields.

The following example shows a possible EP revocation request:

```
<EPCHRevocationRequest>
  <RTID>123-ABCD-4567-89</RTID>
```



```
  <ADSN>2</ADSN>
  <Action>REPLACED</Action>
  <Cause>Member reported card missing</Cause>
</EPCHRevocationRequest>
```

4.6.3.2 CHEP Revocation Response

When the CIMS receives the revocation request, it will verify if the information on record supports revocation (i.e., RT Participant is recognized and has a card) and will then add this RT Participant's card (or the RT Participant) to the revocation list for propagation. The CIMS then returns a status to supply the EP a confirmation of the event. This allows the EP a means of ensuring a revocation is processed without having to examine the revocation list for the card identifier.

In the first of these two examples, the requested card has been marked for replacement and the CIMS responds successfully. In the second, the CIMS responds that card sequence 1 was not recognized as a valid card for this RT Participant.

The XML schema for this message is shown below:

```
<xs:element name="CHEPRevocationResponse" type="RevocationType"/>
```

See above for an explanation of the revocation response fields.

The following shows a possible revocation response:

```
<CHEPRevocationResponse>
  <RTID>123-ABCD-4567-89</RTID>
  <ADSN>2</ADSN>
  <Action>REPLACED</Action>
</CHEPRevocationResponse>

<CHEPRevocationResponse>
  <RTID>A1B2C3D4E5F6G7H8</RTID>
  <ADSN>1</ADSN>
  <Action>NONE</Action>
  <Cause>No such card assigned to RT Participant</Cause>
</CHEPRevocationResponse>
```

4.6.3.3 Notify the TSA of Revocation

Once the CIMS has completed revocation of the card or RT Participant, the CIMS will notify the TSA of this event if the RT Participant is no longer active with any SPs. The CIMS will provide the TSA the global identifier (GUPID) for this RT Participant.

4.7 Card Revocation List Propagation

The RT Program maintains a list of revoked cards as opposed to a list of valid cards. The two primary reasons for this are that over time the RT membership will grow; thus, an active list will become exceptionally large. Also industry standards for card security follow a revocation model instead of an active model.

Once a card has been revoked and is not yet expired, it must be placed on the revocation list. The revocation list in turn must be rapidly distributed to all verification stations to ensure no unauthorized use of a revoked card occurs. The CIMS is responsible for maintaining the revocation list, and the CIMS will distribute it to each VP. The CIMS will distribute the updates on a periodic basis. SPs may request a copy of the CRL if they perceive they have missed an update from the CIMS (the CIMS will not track

which SP has received which update to the list). EPs may also request the list but they are not pushed updates; they must request a copy.

Finally, because the list may become large as the membership in the RT Program fluctuates, both incremental changes and changes to discrete pieces of the complete list have been defined. The CIMS may push changes and a SP may request changes. When the CIMS returns the full content, it may be separated into pieces to support easier delivery. Also, even if an incremental update is requested, the CIMS may return a full content CRL.

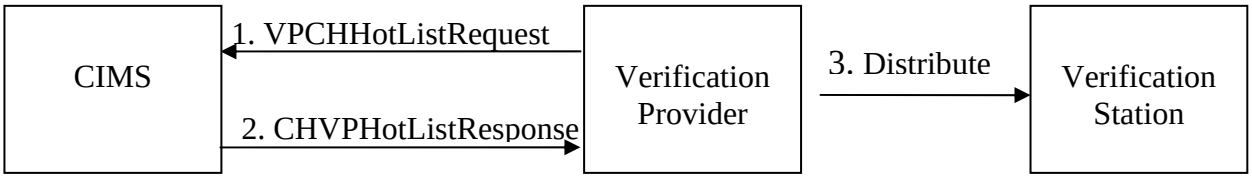


Figure 4-3. Card Revocation List Propagation

4.7.1 VPCH CRL Request

To support requesting a CRL, this message may be sent by a VP or EP to the CIMS. The message specifies which updates are requested or if a complete list is desired. If the requested ID is empty (null), a complete CRL will be returned. If the requested ID is specified, the CIMS will attempt to return only updates that have occurred since the specified ID was sent. It is not possible to request a specific CRL update; instead all updates since the specified point are included. The CIMS may elect to return a complete CRL even if the requested ID is given. VPs must support partial and complete updates. Note too that when a specific update is requested, an empty update may be returned if no changes have occurred since that time. A request with no ID specified will signify that a complete CRL is returned. Note that such a return may be large and should not be performed too frequently.

The XML schema for the CRL request is shown below:

```
<xs:element name="VPCHHotListRequest" type="HotListRequestType">

<xs:complexType name="HotListRequestType">
  <xs:sequence>
    <xs:element name="CRLID" type="IdentifierType" minOccurs="0"/>
  </xs:sequence>
</xs:complexType>
```

<CRLID> Specifies an identifier for a previous CRL that the CIMS can use to determine what updates are needed. This value should not be generated by the VP but is intended to be a copy of the ID for the currently held CRL. As noted previously, the CIMS may elect to return a complete CRL even if a valid CRLID is provided (typically if too many updates have occurred since the identified list was sent out). This element is optional, if not provided then a complete CRL is being requested. Even through this value may appear to be a time-based string, it is a 16-character identifier as defined internally by theCIMS and should simply be retained from a previous CRL.

The following are two example CRL requests is shown below:

```
<VPCHHotListRequest>
  <CRLID>20060602400000001</CRLID>
</VPCHHotListRequest>
```



```
<VPCHHotListRequest>
</VPCHHotListRequest>
```

4.7.2 CHVP CRL Response

This message is used to distribute either updates to or complete contents for a CRL. This is pushed to all VPs by the CIMS. The CIMS may perform this at any time to satisfy the TSA requirement for immediate distribution. This is also returned upon request by an SP. EPs must support requests to add or remove entries that may have been added or removed in prior updates.

The XML schema for a card revocation return response is shown below:

```
<xs:element name=”CHVPHotListResponse” type=”CRLListType”/>
<xs:complexType name=”CRLListType”>
  <xs:sequence>
    <xs:element name=”CRLID” type=”IdentifierType” minOccurs="0"/>
    <xs:element name=”ValidUntil” type="xs:dateTime" minOccurs="0"/>
    <xs:element name=”Complete” type=”xs:boolean” default=”false”
                minOccurs="0"/>
    <xs:element name=”Sequence” type=”xs:string” default=”1:1”
                minOccurs="0"/>
    <xs:element name=”Count” type=”xs:int” />
    <xs:element name="Action" minOccurs=”0”>
      <xs:complexType>
        <xs:sequence>
           <xs:element name="Entry" minOccurs="0"
                       maxOccurs="unbounded">
             <xs:complexType>
               <xs:sequence>
                 <xs:element name="Reason" type="xs:string"
                       minOccurs="0"/>
               </xs:sequence>
               <xs:attribute ref="spid" use="required"/>
               <xs:attribute ref="rtid" use="optional"/>
               <xs:attribute ref="adsn" use="optional"/>
             </xs:complexType>
           </xs:element>
        </xs:sequence>
        <xs:attribute name="type" form="unqualified"
                      type="RevokeActionType" />
      </xs:complexType>
    </xs:element>
    <xs:element name="StatusCode" type="StatusCodeType" />
    <xs:element name="StatusMessage" type="xs:string" minOccurs="0"/>
  </xs:sequence>
</xs:complexType>

<xs:attribute name="spid">
  <xs:simpleType>
    <xs:restriction base="SPIDType" />
  </xs:simpleType>
</xs:attribute>

<xs:attribute name="rtid">
  <xs:simpleType>
    <xs:restriction base="IdentifierType" />
```



```
    </xs:simpleType>
  </xs:attribute>

  <xs:attribute name="adsn">
    <xs:simpleType>
      <xs:restriction base="ADSNType" />
    </xs:simpleType>
  </xs:attribute>
```

<CRLID> Specifies an identifier assigned by the CIMS to this instance of the CRL update. This value is to be retained by the SP to support return of the same value if an update is requested. While the format of this value appears to be date/time based, it should not be considered such. That is, the SP may not generate an ID-based on time expecting to only receive changes since that time. Rather, this allows an SP to request those changes that occurred since a previously received CRL. The suggested format for the CRLID is a time-based CCYYMMDDhhmmss## although SPs should not presume that the format will follow this convention.

<ValidUntil> Specifies the date/time (in Zulu time) that the CRL expires (24 hours from creation) and is used to determine validity of the CRL. This field is required for both full and partial/update CRLs. This field should not be confused with other expiration or validity fields (such as RT card expiration, certificate validity, etc.)

<Complete> Specifies if the given CRL is a complete list or a partial update. This value is optional and implies false or partial update if not specified. This field should not be confused with the sequence value. This value specifies if a complete list is being provided although multiple messages (sequence) may be used to provide it.

<Sequence> Provides a sequence identifier if the CRL has been split into multiple messages to facilitate transfer. The value contains two fields: the first is count, and the second is total, separated with a colon. This element is optional and implies 1:1 (message is not split), if not provided. This field allows an SP to determine which message out of the set of messages is this particular instance. The CRLID would be the same on all messages in the sequence.

<Count> Denotes the total number of CRL entries after all updates have been applied. The total count is the value resulting after both additions and removals from the list.

<Action> Groups the revocation action and provides the type of action as the reason an RT Participant's card or the RT Participant is being revoked.

<Entry> Provides the set of entries on the CRL. All the elements within this set will contain an SPID attribute and may contain the RTID attribute or ADSN attribute. The element also provides an optional reason element to provide a simple explanation as to why an RT Participant is on the permanent revocation list.

The SPID attribute provides an RT Participant's enrollment SP obtained from the card. Note this is the SPID from the card, not the VP ID which would be specified in the header. Note that all cards created by an EP may be revoked by the TSA.

The RTID attribute provides the RT Participant's identifier as specified on the card. This identifier is assigned when the RT Participant is first enrolled by this SP and remains unchanged throughout the association of the RT Participant and the SP. This value allows the CIMS to determine the specific RT Participant's record being referenced. See the description of an identifier in Section 4.3.2, Identifier.

The ADSN attribute specifies the current authentication data sequence number for this RT Participant which may relate to a previously revoked card. This value is specified as a single alphanumeric character.

<StatusCode> provides status codes for the interactions between SPs and the CIMS.

<StatusMessage> provides an optional human readable message related to the StatusCode.

In the first example, SP ZZ has been revoked by the TSA which automatically makes all cards generated by that SP invalid. Also, two other RT Participants for SP AA have been revoked by the TSA. Additionally, two cards from SP “BB” both belonging to the same RT Participant have been replaced and one card for an RT Participant from SP “CC” (presumably card ADSN 1 and 2 have expired in time and do not need to appear). Finally, two RT Participant accounts have expired with SPs DD and EE making all cards assigned to these RT Participants invalid.

In the second example, no CRL entries are returned. This would imply that this is an incremental update (also specified by “false” value for complete) in which no changes have occurred since the previous request. Note the count can be used to determine the total number of entries that should be found on the CRL. If the SP finds this is not consistent with their own list, they can request a full list.

The following is an example CRL content response:

```
<CHVPHotListResponse>
  <CRLID>2006062400000001</CRLID>
  <ValidUntil>2006-06-25T05:00:01Z</ValidUntil>
  <Complete>true</Complete>
  <Sequence>1:1</Sequence>
  <Count>72</Count>
  <Action type="TSA_REVOKED_RTP">
    <Entry spid=”ZZ” />
    <Entry spid="AA" rtid="SS000-1111-2222-33" />
    <Entry spid="AA" rtid="SS000-1111-2222-55" />
  </Action>
  <Action type="REPLACED">
    <Entry spid="BB" rtid="TT12356780123561" adsn="1" />
    <Entry spid="BB" rtid="TT12356780123561" adsn="2" />
    <Entry spid="CC" rtid="AA12356780123599" adsn=”3” />
  </Action>
  <Action type="EXPIRED">
    <Entry spid="DD" rtid="TT123-5678-0123-56" />
    <Entry spid="EE" rtid="AA123-5678-0123-56">
      <Reason>Account not paid</Reason>
    </Entry>
  </Action>
</CHVPHotListResponse>

<CHVPHotListResponse>
  <CRLID>2006062400010001</CRLID>
  <Complete>false</Complete>
  <Count>72</Count>
</CHVPHotListResponse>
```

4.7.3 VP Distribution of CRL

Once the VP has received the CRL, it must be distributed to the individual verification stations. How and at what frequency this content is distributed does not affect interoperability other than the requirement for

the VP to meet all security and business obligations. The above definitions can be used or the VP may determine their own method of formatting. The informational content must be provided without alteration for the verification stations to use in performing card validation.

4.8 Active Applicant Consistency Check

Because RT Applicants enter and leave the program at random time periods, and memberships may be suspended or restored, there is concern that over extended time periods, the actual list of applicants may get "out-of-sync" between the EPs and the CIMS. For this reason, an applicant consistency check operation is implemented. On a periodic basis (potentially monthly), all EPs are required to generate a list of their presently known members and submit the list to the CIMS. The CIMS will in turn cross reference these with its record of applicants for that EP and notify the EP of discrepancies which can then be resolved. Resolution of discrepancies is presently expected to be handled manually.

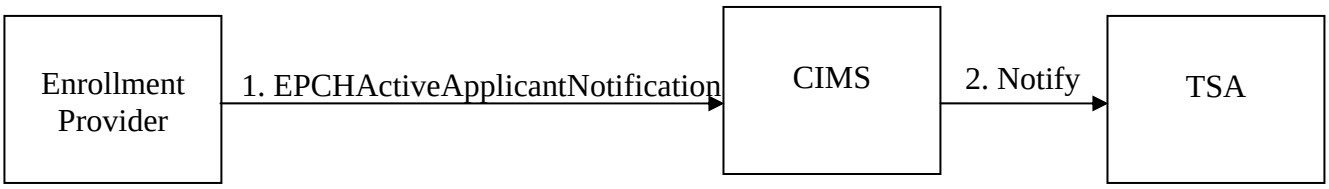


Figure 4-4. Participant Consistency Check

4.8.1 EPCH Active Applicant Notification

This message is sent from each EP to the CIMS and contains a current list of applicants. The CIMS will work with the TSA and the EPs to ensure active participant synchronization.

Due to similarities in message content, this message is formatted similarly to the CRL, although the SPID is not needed and a different set of states exist. Because of the potentially large number of participants, this message may be split into multiple sub-messages. The EP should specify the total number of applications on which they are reporting across all sub-messages in the count field and use the sequence field to record which piece of the data is being sent.

The EP must also ensure that this list of participants contains only those that have been submitted to the CIMS at the time of message submission. That is, if the EP is actively adding new participants while this message is being generated, the message must contain only those participants that have been submitted to the CIMS for enrollment. This may require the EP to temporarily delay submission of new enrollments until this active participant list has been sent to the CIMS.

The XML schema for the active applicant message is shown below:

```
<xs:element name="EPCHActiveApplicantNotification"
type="ActiveListType"/>
<xs:complexType name="ActiveListType">
  <xs:sequence>
    <xs:element name="Count" type="xs:int"/>
    <xs:element name="Sequence" type="xs:string" default="1:1"/>
    <xs:element name="State" maxOccurs="unbounded">
      <xs:complexType>
        <xs:sequence>
```



```
            <xs:element name="Entry" minOccurs="0" maxOccurs="unbounded">
              <xs:complexType>
                <xs:attribute ref="rtid"/>
                <xs:attribute ref="adsn" use="optional"/>
              </xs:complexType>
            </xs:element>
          </xs:sequence>
          <xs:attribute name="type"
                        type="ApplicantStateType" form="unqualified"/>
        </xs:complexType>
      </xs:element>
    </xs:sequence>
  </xs:complexType>
```

<Count> Specifies the total number of applicants in the complete list managed by the EP. This value is independent of the number of messages used to pass this content to the CIMS.

<Sequence> Provides the number of messages used and the sequence in which this specific message occurs. This allows the CIMS to recognize when all messages have been received from an EP.

<State > Provides a grouping for a state of applicants. Within this list, all applicants on record with the specified applicant state are listed. Multiple state groupings are used to accommodate all potential conditions within the applicants on record. The attribute “type” is used to specify the actual applicant state being considered in Section 4.3.5, Applicant State.

<Entry> Provides the applicant’s RTID and ADSN being referenced. The RTID will always be specified. The ADSN is provided only when a card is being referenced (for active and suspended entries). These values are specified through the XML attributes “RTID” and “ADSN”.

In the example below, the total number of participants is six, as denoted by the count value. The entire list is being submitted in one message, as noted by the sequence value. There are two active participants with their ADSNs; a third submitted to CIMS pending their STA; another with a suspended card; a fifth with an expired account (still within 90 days and not yet “off-the-books”); and finally a sixth applicant that was revoked by the TSA. This list provides all EP applicants that have been provided to the CIMS.

The following example shows a possible active participant list:

```
<EPCHActiveApplicantNotification>
  <Count>6</Count>
  <Sequence>1:1</Sequence>
  <State type=″ACTIVE″>
    <Entry rtid=″1234-ABCDE-012982″ adsn=″3″ />
    <Entry rtid=″9726-OJSUE-681823″ adsn=″1″ />
  </State>
  <State type=″PENDING″>
    <Entry rtid=″8172-AAMCH-827382″ />
  </State>
  <State type=″SUSPEND″>
    <Entry rtid=″8162-VCEWS-728389″ adsn=″1″ />
  </State>
  <State type=″EXPIRED″>
    <Entry rtid=″2732-JXJIW-728382″ />
  </State>
  <State type=″TSA_REVOKED_RTP″>
    <Entry rtid=″1000-AAAAA-000001″ />
```



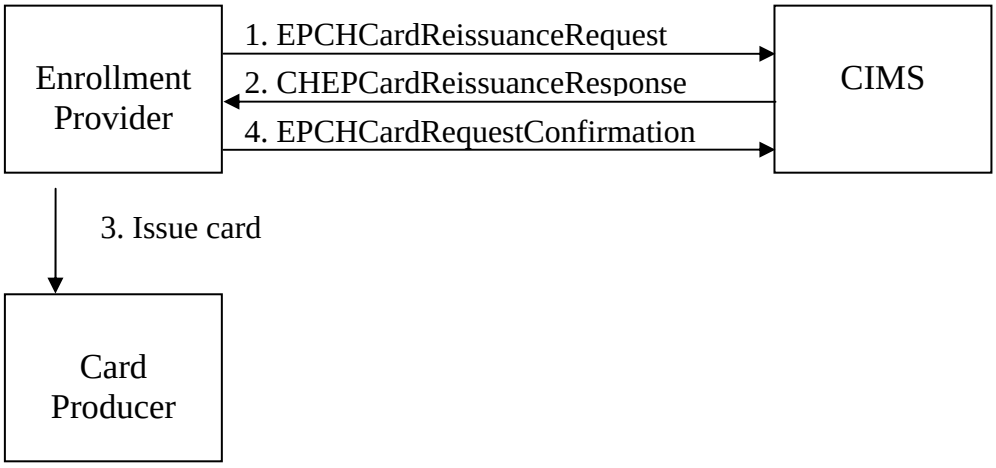
```
  </State>
</EPCHActiveApplicantNotification>
```

4.8.2 Notify

Upon receipt of the active applicant list from the EP, the CIMS will correlate this against the information it holds on each applicant. Discrepancies will be noted and the CIMS will then contact the EP and together they will determine the cause of the differences. A report on the problems and corrections will then be provided to the TSA.

4.9 Card Re-issuance

Card re-issuance is used to provide a replacement card for an RT Participant. The following flow diagram shows the processing stages between the EP and the CIMS. This flow addresses only issuing a new card. Revocation of any prior cards for the same RT Participant is shown in the Section 4.6.3,



Revocation of RT Participant by Enrollment Provider.

Figure 4-7. Card Re-Issuance

4.9.1 EPCH Card Re-issuance Request

This message is sent from an EP to the CIMS to request the authentication payload for a new card.

The schema definition for this message content consists of three required elements:

```
<xs:element name="EPCHCardReissuanceRequest" type="CardRequestType"/>

<xs:complexType name="CardRequestType">
  <xs:sequence>
    <xs:element name="RTID" type="IdentifierType" />
    <xs:element name="RequestedFingers" type="RequestedFingersType"
                minOccurs="0" />
  </xs:sequence>
</xs:complexType>
```


<RTID> Provides the RT Participant's identifier as determined by the SP. This identifier is assigned when the RT Participant is first enrolled by this EP and remains unchanged throughout the association of the RT Participant and the SP. This value allows the CIMS to determine the specific RT Participant's record being referenced. See the description of an identifier in Section 4.3.2, Identifier.

<RequestedFingers> Provides the desired fingers for this RT Participant. This allows a change over the original fingers on previous cards if desired by the RT Participant. The CIMS may not be able to support the specified biometrics; the EP must actually use the fingers returned as part of the payload (see Section 4.9.2, CHEP Card Re-issuance Response).

The following example shows a possible EP re-issuance request:

```
<EPCHCardReissuanceRequest>
  <RTID>A1B2C3D4E5F6G7H8</RTID>
  <RequestedFingers>2,3,6,7</RequestedFingers>
</EPCHCardReissuanceRequest>
```

4.9.2 CHEP Card Re-issuance Response

Once the CIMS has generated the new card payload, it is returned to the EP to allow writing it to a card. This message provides the necessary information generated by the CIMS in separate fields to allow the EP to separate this as necessary in communicating with the card issuer. The EP must take care that the values are not altered to avoid verification failures. Note that the content for this message is encrypted when being returned to the EP.

The schema definition for this message content is defined below:

```
<xs:element name="CHEPCardReissuanceResponse"
type="CardReIssuanceType"/>

<xs:complexType name="CardReIssuanceType">
  <xs:sequence>
    <xs:element name="RTID" type="IdentifierType" />
    <xs:element name="ADSN" type="ADSNType" minOccurs="0"/>
    <xs:element name="Expire" type="xs:date" minOccurs="0"/>
    <xs:element name="Payload" type="AuthPayloadType" minOccurs="0"/>
    <xs:element name="StatusCode" type="StatusCodeType"/>
    <xs:element name="StatusMessage" type="xs:string" minOccurs="0"/>
  </xs:sequence>
</xs:complexType>
```

<RTID> The RT Participant identifier as specified by the EP in the original request. This is returned to provide context for the EP allowing association with the original request. This is an identifier as described in Section 4.3.2, Identifier.

<ADSN> The newly assigned authentication data sequence number to be used for this card. This value is a single alphanumeric character.

<Expire> Provides the expiration date for the new card as managed by the CIMS. This value can be retained by the SP to record the card expiration date which may be different from the RT Participant's enrollment period with the EP. When this date is reached, the CIMS will automatically expire the card; a new card must be issued prior to this date to remain active. This value is a date string specifying century, year, month, and day of expiration.

<CardKeys> Provides the derived key for the card based on the derivation data and the master key.

<Payload> Specifies the various elements that must be placed on the RT Participant's card. This is further broken into child elements to allow easier interaction between the EP and the card issuer. The EP must ensure these data elements are placed on the card without modification. The EP must also build and sign the card identifier field which is constructed of various ID fields.

<StatusCode> provides status codes for the interactions between SPs and the CIMS.

<StatusMessage> provides an optional human readable message related to the StatusCode.

The following example shows a possible card re-issuance response:

```
<Content>
  <EncryptedData Id="DOC" xmlns="http://www.w3.org/2001/04/xmlenc#"
          Type="http://www.w3.org/2001/04/xmlenc#Content">
    <EncryptionMethod
          Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:RetrievalMethod URI="#KEY"
          Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey"/>
      <ds:KeyName>TemporaryKey</ds:KeyName>
    </ds:KeyInfo>
    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <EncryptedKey Id="KEY" xmlns="http://www.w3.org/2001/04/xmlenc#">
        <EncryptionMethod
            Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
        <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
          <ds:KeyName>ProviderKey</ds:KeyName>
        </ds:KeyInfo>
        <CipherData>
          <CipherValue>encrypted+key</CipherValue>
        </CipherData>
        <ReferenceList><DataReference URI="#DOC"/></ReferenceList>
        <CarriedKeyName>TemporaryKey</CarriedKeyName>
      </EncryptedKey>
    </ds:KeyInfo>
    <CipherData>
       <CipherValue>base64+encrypted+content</CipherValue>
    </CipherData>
  </EncryptedData>
</Content>
```

Where the encrypted data content after decryption would contain the following:

```
<CHEPCardReissuanceResponse>
  <RTID>A1B2C3D4E5F6G7H8</RTID>
  <ADSN>3</ADSN>
  <Expire>2010-06-28</Expire>
  <CardKey>base64+content</CardKey>
  <Payload>
    <FingerprintObjectOne>base64+content</FingerprintObjectOne>
    <FingerprintObjectTwo>base64+content</FingerprintObjectTwo>
    <IrisObject>base64+content</IrisObject>
    <FacialObject>base64+content</FacialObject>
    <PersonalDataObject>base64+content</PersonalDataObject>
    <SecurityDataAuthObject>base64+content</SecurityDataAuthObject>
  </Payload>
</CHEPCardReissuanceResponse>
```


4.9.3 Issue Card

This step denotes the EP sending the payload data to the card issuer. Since EPs may not themselves actually produce the cards, this step recognizes this level of separation. The actual content of any message and format thereof is determined by the SP. Multiple interchanges are allowed and the EP may batch a series of card productions into a single request/response cycle. How the message is transferred is also at the determination of the SP although all RT level security requirements must be satisfied.

While the actual content of the message can be defined by the SP, there are specific data items returned by the CIMS that must be transferred to be placed on the card. These items are the RTID, ADSN, Expired, and the Payload fields. The EP must also generate a digital signature that can be used to authenticate that the EP created the various fields.

4.9.4 EPCH Card Request Confirmation

The payload acknowledgement is returned by the EP to the CIMS to signify that the card payload has been successfully received and that the CIMS can delete the biographic data.

The XML schema for a verification notification is shown below:

```
<xs:element name="EPCHCardRequestConfirmation"
type="PayloadAcknowledgementType" />
```

The following example shows an example verification notification:

```
<EPCHCardRequestConfirmation>
  <StatusCode>OK<StatusCode>
</EPCHCardRequestConfirmation>
```

5 The RT Card

The Registered Traveler system requires a common smart card specification enabling all accredited SPs to issue credentials to approved RT Applicants and to authenticate individuals at verification checkpoints. The RT card application is defined as a distinct and standalone application. A fundamental business consideration guiding the development of this application definition is the notion that RT checkpoint processing may only rely upon the information contained within the RT application space. RT processing is further specified to not rely upon information obtained from any other application space.

This card model is based upon the PIV endpoint specification as defined by NIST SP 800-73. The transitional interface is specifically excluded. It was not possible to use the SP800-73 documentation directly as there are conflicts with its name space assignments, data model, and access control rules. Essentially, the card edge was maintained with an RT-specific data model introduced.

5.1 RT Card Application

The RT system is based on the RT Card Application, which is stored in the smart card. The RT Card Application supports card command interfaces described in the following sections. Each card command performs operations on and with the data objects to which the RT Card Application has access.

Each card application stored in the smart card has a globally unique identifier, the Application Identifier (AID). Access to the card commands and data objects of a card application shall be gained by selecting the card application using its application identifier.

The AID of the RT Card Application shall be:

A0 00 00 03 48 00 00 00 01 00 01

The AID of the RT Card Application consists of the RTIC Registration ID (RID) (A0 00 00 03 48) followed by the application portion of the RTIC Proprietary Application Identifier Extension (PIX) indicating the RT Card Application (00 00 00 01) and then the version portion of the RTIC PIX (00 01) for the first version of the RT Card Application. All other PIX sequences on the RTIC RID are reserved for future use.

5.2 RT Application Interfaces and Namespaces

There are two types of interfaces to a smart card application: high-level client Application Programming Interfaces (API) and a low-level Card Command Interface (card edge). Both interfaces can be implemented by a collection of software modules collectively treated as middleware.

The client API provides task-specific programmatic access to these concepts and constructs and the card command interface provides communication access to concepts and constructs. The client API is used by client applications using the RT Card Application. The card command interface is used by software implementing the client API (middleware).

The client API is considered to be at a higher level than the card command interface because access to a single entry point on the client-application programming interface may cause multiple card commands to traverse the card command interface. In other words, it may require more than one card command on the card command interface to accomplish the task represented by a single call on an entry point client API.

The RT interface is a simplified version of the interface specified by NIST SP 800-73, and is intended for implementation at the card command interface. The RT application namespace is defined only by Basic Encoding Rules – Tag Length Value (BER-TLV) tags. Should a PIV middleware approach be desirable,

this specification provides an API definition that is a variation of pivGetData that uses the BER-TLV tag instead of an Object Identifier (OID).

5.3 RT Data Model

5.3.1 RT Data Objects (Containers) and Contents

RT Card Application shall contain the following data objects:

RT Data Object	Max. Bytes	Read Access Rule	BER TLV Tag on Card Edge	Object and Group
RTUID	1410	Always	FF A1 01	1
Fingerprint I	2004	Mutual Authenticate	FF A1 02	2
Fingerprint II	2004	Mutual Authenticate	FF A1 03	3
Iris Biometrics	8008	Mutual Authenticate	FF A1 04	4
Facial Image	17104	Mutual Authenticate	FF A1 05	5
Personal Data	74	Mutual Authenticate	FF A1 06	6
RT Preferences	8	Always	FF A1 07	7
ICAO Security Object	1504	Always	FF A1 11	11

Table 5-1. RT Containers

All data objects are mandatory. Some elements in the personal data and RT preference objects are optional. None of the objects may be updated after creation. All multi-byte objects are big endian unless otherwise specified.

Note: The Answer to Reset (ATR) card capabilities data coding byte, bit 5, should be set to 1, indicating that the ‘FF’ for the first byte of the BER-TLV tag field is valid.

5.3.2 Registered Traveler Unique Identifier (RTUID) Object

RTUID is the object used for the unique identification of the RT card and its issuer. The Payload ID inside the RTUID object is signed by the CIMS through the security object. The RTUID is signed by the EP.

Data Element (TLV)	Tag	Type	Max. Bytes
Payload ID (see table 5-3)	0x80	Fixed text	27
Verification ID (VID)	0x81	Fixed text	16
Authentication Key Version	0x82	Fixed	1
Enrollment Provider Asymmetric Signature	0x85	Variable	1356

Table 5-2. RTUID Definition

Data Element	Length
Service Provider ID (SPID)	2 bytes
Registered Traveler ID (RTID)	16 bytes
Authentication Data Sequence Number (ADSN)	1 byte
Expiration Date	8 bytes (Format: YYYYMMDD)

Table 5-3. Payload ID Definition

The SPID is a two- character field that identifies an SP. Every SP participating in the RT program will be assigned a unique SPID.

The RTID is an SP-assigned 16-character field that uniquely identifies participants within an SP domain. Its format consists of 0-9, A-Z (upper case only), _ (underscore), and – (dash) only.

The ADSN is assigned by the CIMS and identifies the Payload sequence as issued by the CIMS. This number is incremented every time the CIMS issues a new payload for an RT Participant, which is typically a result of a re-issuance request from an SP. This is a one character field.

The combination of the SPID, RTID, and ADSN uniquely identifies a card.

The expiration date is an eight- character field with the format YYYYMMDD.

The VID is an anonymous identifier captured at the verification stations for inter-SP billing purposes.

The Authentication Key Version is binary and indicates which key version should be used in performing Card Mutual Authentication.

The Asymmetric Signature data element of the RTUID shall be encoded as a Cryptographic Message Syntax (CMS) external digital signature, as defined in RFC 3852. The digital signature shall be computed over the entire contents of the RTUID, excluding the Asymmetric Signature field.

5.3.3 Fingerprint I Object

The Fingerprint I object contains two fingerprint templates. Both fingerprint templates will be stored in a single INCITS 378-2004 data interchange format with a CBEFF header as received from the CIMS.

Biometric data format and header details are found in Section 3, Biometric Data Management and Use. Integrity and binding to the credential is enforced by the Security object.

Data Element (TLV)	Tag	Type	Max. Bytes
INCITS 378-2004 w/ CBEFF header	0x80	Variable	2000

Table 5-4. Fingerprint I Object

5.3.4 Fingerprint II Object

The second fingerprint data object contains up to two additional fingerprint templates which will be stored in a single INCITS 378-2004 data interchange format with a CBEFF header as received from the CIMS.

Biometric data format and header details are found in Section 3, Biometric Data Management and Use. Integrity and binding to the credential is enforced by the Security object.

Data Element (TLV)	Tag	Type	Max. Bytes
INCITS 378-2004 w/ CBEFF header	0x80	Variable	2000

Table 5-5. Fingerprint II Object

5.3.5 Iris Biometrics Object

This object contains up to two polar images, if available. Its format will be based on the ISO/IEC 19794-6:2005 standard with a CBEFF header as received from the CIMS. The iris images will be stored in separate CBEFF records. Biometric data format and header details are found in Section 3, Biometric Data Management and Use. Integrity and binding to the credential is enforced by the Security Object.

Data Element (TLV)	Tag	Type	Max. Bytes
ISO 19794-6 Iris Image w/ CBEFF Header	0x80	Variable	4000
ISO 19794-6 Iris Image w/ CBEFF Header	0x81	Variable	4000

Table 5-6 Iris Object

5.3.6 Facial Image Object

This object contains an electronic facial image stored in the INCITS 385-2004 format.

Biometric data format and header details are found in the Section 3, Biometrics Data Management and Use. Integrity and binding to the credential is enforced by the Security Object.

Data Element (TLV)	Tag	Type	Max. Bytes
Facial Image - ANSI/INCITS 385 data w/ CBEFF header	0x80	Variable	17100

Table 5-7. Facial Image Object

5.3.7 Personal Data Object

This object shall contain personal data such as first and last name, as well as the order in which the biometrics are stored in the containers. Table 5-9, Biometric Mapping Description, describes which biometrics are stored in the corresponding containers.

Data Element (TLV)	Tag	Type	Max. Bytes
First Name	0x80	Variable text	20
Middle Name	0x81	Variable text	20
Last Name	0x82	Variable text	20
Biometric Mapping (see table below)	0x83	Fixed numeric	6

Table 5-8. Personal Data Object

Biometric Matching Description		Offset
FP 1	1st finger stored in Fingerprint I object	0x00
FP 2	2nd finger stored in Fingerprint I object	0x01
FP 3	1st finger stored in Fingerprint II object	0x02
FP 4	2nd finger stored in Fingerprint II object	0x03
IRIS 1	1st iris stored in Iris object	0x04
IRIS 2	2nd iris stored in Iris object	0x05

Table 5-9. Biometric Mapping Description

The biometric mapping information is returned with the biometric payload from the CIMS. The identifier values for each biometric position are in Table 5-10, Biometric Identifiers. These identifiers are defined in INCITS 398-2005, Common Biometric Exchange Formats Framework, Table 6.

Biometric Identifiers	Value
Null	0x00
Right Eye	0x01
Left Eye	0x02
Right Thumb	0x05
Left Thumb	0x06
Right Index	0x09
Left Index	0x0A
Right Middle	0x0D
Left Middle	0x0E
Right Ring	0x11
Left Ring	0x12
Right Little	0x15
Left Little	0x16

Table 5-10. Biometric Identifiers

5.3.8 RT Preferences Object

The RT Preferences Object contains the biometric preferences and optional interaction language preferences fields.

The biometric preferences are required and specify which biometric to present to the verification station. The verification station may choose to ask initially for the primary biometric, or present a listing of available biometrics as long as the primary exists in this list. The first byte of the preferences field is the primary biometric and the second byte indicates the secondary biometric.

The interaction language preference is optional and shall default to English if it is not specified or if the specified language is not supported.

Data Element (TLV)	Tag	Type	Max. Bytes
Biometric Preferences	0x80	Fixed	2
Interaction Language (optional)	0x81	ISO 639-1 two letter code. (“en”= English)	2

Table 5-11. RT Preferences Object

5.3.9 ICAO Security Object

The CIMS shall sign the security object.

This object is used as the container for the group signature of hashes of all data objects that are authenticated by the CIMS. All RT data objects that are authenticated are done so indirectly through the signature of the ICAO Security Object.

The ICAO Security Object is in accordance with Appendix C.2 of PKI for Machine Readable Travel Documents (MRTD) Offering ICC Read-Only Access Version 1.1. The 16 Data Groups (DG) specified by the MRTD correspond to the last byte of the RT Data Object’s BER-TLV tag. As a special case, the hash of the RTUID (Group 1) only contains the 27 bytes of the Payload ID. The hashes of the other objects include the tags and lengths of each part of the object per PIV. For example, the Fingerprint I container would correspond to DG2, as the RT Data Objects BER-TLV tag is FF A1 02. The SignedMessage includes the message and the certificate of the signer. This allows the Security object to be checked without reading all the RT data objects, and then each hash can be relied upon to validate the data objects processed. This enables the ICAO Security Object to be fully compliant for future activities with identity documents.

Data Element (TLV)	Tag	Type	Max. Bytes
ICAO Security Object	0x80	Variable	1500

Table 5-12. ICAO Security Object

5.3.10 Optional Data Objects

Two types of optional data objects are defined for use within the RT card model.

- Objects with formal definition within the RT schema, with implementation rules being optional.
- Objects with no definition within the RT schema, with implementation rules being optional and at the SP's discretion.

The object defined with formal definition is the Application Information Object. The Application Information Object will exist with tag FF A1 41.

The only object defined as open, SP-specific use, is the SP Specific object. If used, it will exist with tag FF A1 61.

This optional object can be used for any SP-specific function. RT allocates a tag simply to inform SPs what tag they should use if they implement SP-specific features.

Future versions of the RT Data model may include the addition of, modification to, or deletion of data objects and/or data elements within objects.

Note: Optional RT objects (0x40-0x5F) and SP specific RT objects (0x60-0x7F) are never part of the Security object. These are under the control of the SP and are not signed by the CIMS.

5.3.10.1 Application Information Object

This object contains information regarding the application provider and specific build/version of the card application itself. Integrity and binding to the credential is not enforced.

Data Element (TLV)	Tag	Type	Max. Bytes
Application Provider Name	0x80	Fixed text	6 (ASCII characters)
Version	0x81	Fixed	3

Table 5-13. Application Information Object

The RT Card Application provider tells who implemented this RT Card Application; for example, "Gizmos." Note that the RT Card Application provider name is limited to six characters and is left justified within the fixed length field. The version is made up of the major version, the minor version, and the build number; for example, 0x01 0x02 0x07 would be version 1.2 and build 7.

5.3.10.2 Service Provider Specific Data Object

This object contains SP-specific data. This object is managed completely by the SP and may be restructured (to add sub-fields, for example) by the SP, as appropriate. Integrity and binding to the credential is not enforced.

Data Element (TLV)	Tag	Type	Max. Bytes
Service Provider Data	0x80	Variable	TBD

Table 5-14. Service Provider Information Object

5.3.11 Notes on the BER-TLV Tags of the RT Data Objects

This section explains how the object BER-TLV tags are calculated. This information is originally provided in the NIST SP 800-73 namespace origin section.

First the BER-TLV tag definition for a three byte tag is:

```
c c p f f f f f   1 t t t t t t t   0 t t t t t t t   = BER tag definition
0 0                                                  = universal class
0 1                                                  = application class
1 0                                                  = context specific
1 1                                                  = private class
    0                                                = primitive
    1                                                = constructive
      1 1 1 1 1                                      = multi-byte tag
```

Since RT is using the private class of tags, constructed from more BER-TLVs, all the RT tags are:

```
c c p f f f f f   1 t t t t t t t   0 t t t t t t t   = BER tag definition
1 1 1 1 1 1 1 1                                      = priv,cons,multi-byte
```

The tag number is in the 14 bits of `ttttttt ttttttt`.

The PIV convention allocates the 14 tag bits as follows:

```
c c p f f f f f   1 t t t t t t t   0 t t t t t t t   = BER tag definition
c c p f f f f f   1 m m v v v v v   0 n n n n n n n   = BER tag + PIV map
                    m m                              = data model
                        v v v v v                    = object version
                                    n n n n n n n    = object number
```

This is the first RT data model and all objects are first version:

```
c c p f f f f f   1 m m v v v v v   0 n n n n n n n   = RT bit def. so far.
1 1 1 1 1 1 1 1   1 0 1 0 0 0 0 1                    = 0xFF 0xA1 ...
```

The RT convention is to further assign object numbers to the different types of RT objects:

```
c c p f f f f f   1 m m v v v v v   0 n n n n n n n
1 1 1 1 1 1 1 1   1 0 1 0 0 0 0 1   0 0              = mandatory RT objects
```

```
1 1 1 1 1 1 1 1   1 0 1 0 0 0 0 1   0 1 0           = optional RT objects
1 1 1 1 1 1 1 1   1 0 1 0 0 0 0 1   0 1 1           = SP specific objects
```

The mandatory RT objects will have BER-TLV tags from FF A1 01 to FF A1 3F.

5.4 Client Application Programming Interface

If an SP wishes to use the PIV middleware API on an RT card, a natural extension would be the API below that provides a simple variation of pivGetData that uses the BER-TLV tag instead of the OID.

pivGetDataByTag

Purpose: Return the entire data content of the named data object.

Prototype: status_word **pivGetDataByTag**(

IN handle **cardHandle**,

IN sequence of byte **BER-TLV-TAG**, //Replaces OID

OUT sequence of byte **data**

);

Parameters:

cardHandle Opaque identifier of the card to be acted upon as returned by pivConnect.

BER-TLV-TAG The BER-TLV tag of the object whose data content is to be retrieved. For example, 'FFA105'.

data Retrieved data content.

Return Codes:

`PIV_OK`

`PIV_INVALID_CARD_HANDLE`

`PIV_DATA_OBJECT_NOT_FOUND`

`PIV_SECURITY_CONDITIONS_NOT_SATISFIED`

`PIV_CARD_READER_ERROR`

5.5 Card Command Interfaces

In the RT system, Card Command Interfaces are adopted from the FIPS 201 standard without any modifications. The following Card Commands are the only commands utilized by the RT application:

Command	Example	Security Condition for Use	Command Chaining	Notes
SELECT	`00 A4 04 00 0B` `A0 00 00 03 48 00 00 00 01 00 01`	Always	No	The contents of the response are not considered in RT interoperability.
GET DATA	`00 CB 3F FF 05` `5C 03 FF A1 01`	Data dependent	No	Read the RTUID.

GENERAL AUTHENTICATE	00 87 01 9F 04 7C 02 80 00	Always	No	Request a witness (8 bytes in length).
GENERAL AUTHENTICATE	00 87 01 9F 16 7C 14 80 08 dw dw dw dw dw dw dw dw 81 08 pc pc pc pc pc pc pc pc	Always	No	Send decrypted witness and plaintext challenge value.

Table 5-15. Card Commands

5.6 Card/Verification Station Authentication and Key Management

This section explains how cards and verification stations mutually authenticate, and how the needed keys are created, distributed, and used. Please refer to Section 6, System Security, for detailed information.

Mutual Authentication (MA) enables the card and the verification station to each know that the other is a legitimate part of the RT system. The card should verify that the verification station is legitimate so that the card does not release the cardholder's biometrics to outside parties. The verification station should verify that the card is valid so that it does not allow cards that were not issued by a trusted SP to be used for verification.

5.6.1 RT Card-Verification Station Authentication Summary

The RT card and verification station share a symmetric key which is used for mutual authentication. This master key is generated by the CIMS and securely distributed to valid RT VPs who utilize it for mutual authentication purposes.

Each card issued by a certified EP will contain a card key derived from the master key. The card key will prevent sensitive data on the RT card from being read by unauthorized parties. The purpose of deriving card keys from one master key is to lessen the impact on the RT system should one card key be disclosed; gaining knowledge of one card key does not allow an attacker to gain control over other cards.

Upon certification of a VP, the CIMS will distribute the master key in an HSM. Master keys will be updated on a pre-defined schedule to minimize the population of cards affected in the unlikely case that a single master key is compromised. As new master keys are distributed, the version number will be updated. VPs will need to authenticate each card using the appropriate master key. The version number for a particular card is stored in the RTUID object.

5.6.2 Algorithm Identifier

An algorithm identifier shall be a one-byte identifier of a cryptographic algorithm together with a mode of operation and reference data length. The table below lists the algorithm identifier for the cryptographic algorithm recognized on the RT interfaces. All other algorithm identifier values are found in publication NIST SP 800-78-1 and are reserved for future use.

Algorithm Identifier	Algorithm – Mode	Reference Data Length	M/O
01	2 Key Triple DES – ECB	128 bits	M

Table 5-16. Cryptographic Algorithm Identifier

The default cryptographic algorithm for the RT Card Application with algorithm identifier '01' is 2 Key Triple DES - ECB.

5.6.3 Key References

A key reference is a six-bit identifier of cryptographic material in the RT Card Application used in a cryptographic protocol. When represented as a byte, the key reference occupies b8 and b5-b1, while b7 and b6 shall be set to 0. If b8 is 0, then the key reference names global reference data. If b8 is 1, then the key reference names application-specific reference data.

The table below defines the key reference value that shall be used for RT MA. All other key reference values are reserved for future use.

This key is used for card-to-verification station MA purposes. Please refer to Section 5.7.8, Mutual Transaction Authentication with Card, for additional detail.

Algorithm Identifier	Key Reference Value	Key Reference Name	Authenticatable Entity	Security Status	Retry Reset Value	Number of Unblocks
01	9F	Mutual Authentication Key	Verification station <-> Card	Application	N/A	N/A

Table 5-17. Card Application Authentication Algorithm Identifier

5.6.4 Key Notation and Derivation

The RT system uses the following keys and data for mutual authentication:

Key Symbol	Meaning	Locations
KM[version]	Master Key: A 16 byte, Triple DES ECB (2 KEY mode), key used to derive the card keys. Over time, there will be multiple KMs indexed by a version. The KM is only stored within a secure device.	CIMS holds all KMs. Each verification provider's verification station has all the valid KMs in a secure device.
DD	Derivation Data = Payload ID = SPID | RTID | ADSN | Expiration.	Readable from each RT card's RTUID.
KC	Card Keys = derived from the KM and derivation data.	Stored on each card securely during card personalization
Version	An index into an array of master keys.	Readable from each RT card's RTUID.

Table 5-18. Key Notation

Note: For security purposes, the specific KC derivation mechanism (while fully documented) is only shared on a need to know basis. Please contact the RTIC if you need this information.

5.6.5 Origin and Distribution of Versioned Master Keys

The CIMS will generate the versioned KMs, insert them into the devices, and distribute the devices to the verification SPs. As a standard rule, a new KM will be distributed to SPs every two years or for every 1 million cards issued, whichever is greater. Alternately, a new KM may be securely transmitted to devices

installed in the field. The CIMS will distribute a device to a newly certified verification SP. Please refer to Section 6, System Security, for additional information regarding management of the KM.

There is a version associated with each KM so that not all of the cards' KC values are derived from the same key. In the event of a particular KM disclosure, then the RT program has the option of only revoking some of the cards. Even if the RT program decides not to revoke existing cards, it can create a new KM, and after all of the old KM cards have expired, remove the old KMs from the verification stations.

5.6.6 Use of KM by Enrollment Providers

Enrollment SPs will not directly utilize the KM. The CIMS will perform the derivation routine and generate the KC to be encoded into the RT cards during personalization. The KC and related version number will be delivered as a part of the CIMS payload.

5.6.7 Use of KM by Verification Providers

When a VP receives the KM device, they will install it on their verification stations. Details on hardware device requirements are found in Section 5.7.9, Verification Station KM Storage Device Specifications.

5.6.8 Mutual Authentication Transaction with Card

Mutual authentication is achieved by using the "General Authenticate" card command from SP 800-73's PIV final card edge.

The following are the card commands and responses needed to perform the mutual authentication.

00 87 01 9F 04	Command = General Authenticate
7C 02 80 00	Request an encrypted witness value from the card.
7C 0A 80 08	Response =
92 26 73 13 F9 0B 14 28	encrypted witness
90 00	

_____

Decrypt the witness (in this case, 92 26 73 13 F9 0B 14 28) using the card key and send it and a plaintext challenge value (in this case, 01 02 03 04 05 06 07 08) to the card.

00 87 01 9F 16	Command = General Authenticate
7C 14 80 08	
95 64 DE 6B 6D D1 EB B4	witness (prove that the terminal knows the key)
81 08	
01 02 03 04 05 06 07 08	plaintext challenge value

7C 0A 80 08	Response =
C2 FB 2C FD 10 73 05 A8	encrypted challenge (prove that the card knows the key)
90 00	

Decrypt the encrypted challenge (in this case, C2 FB 2C FD 10 73 05 A8) using the card key and check that it matches the plaintext challenge value.

The following is the triple DES key used in the previous example:

11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF 00

The following figure depicts the mutual authentication process between the card and the Secure Access Module (SAM).

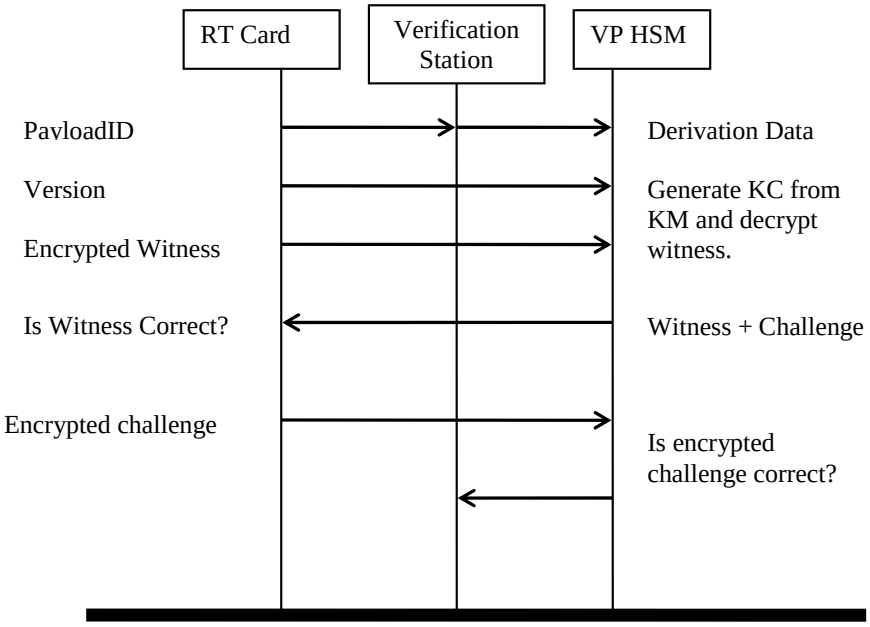


Figure 5-1. Card-SAM Mutual Authentication

5.6.9 Verification Station KM Storage Device Specifications

For greater security, the KM will be stored in a hardware device such as a smart card or USB token so that the KM cannot be read, but the device can be used to authenticate with the card.

The device must support the following specifications for use by the verification provider in the verification station:

- Must be a hardware platform conforming to the FIPS 140 Level 2 certification standards.
- The device accepts a KM and version or multiple instances of KM and version. The device stores the KM[version] in nonvolatile memory.

- The verification station activates the device using MA. Device refuses to operate further until the MA is successful. The device stays active until it loses power.
- Verification station submits version, derivation data (DD), and encrypted witness to device. The device derives the KC from the KM and DD. The device generates and holds an eight byte random challenge. The device returns the witness and the challenge values to the verification station.
- Verification station submits an encrypted challenge to the device. The device decrypts the challenge and compares it to the held challenge. The device returns TRUE if the challenges match, indicating the card is legitimate.
- A KM[version] can be deleted, thus preventing any further verification of this version of KM.
- The device can hold a minimum of 20 KMs.

5.7 Physical Card Requirements

5.7.1 Card Topology

Physical card topology is unique to each service provider within the following guidelines. These guidelines provide flexibility for competitive design decisions within a framework that allows TSA and other service providers to securely and accurately identify a valid card via a visual inspection at the verification lane.

Guidance from the TSA as of this version of the specification is as follows:

- The facial photograph is optional on the outside of the card.
- TSA requires the following language to appear on all cards issued for the RT Program: “This is not a government identification card.”
- The Registered Traveler logo must appear on the card.
- The full name (first name, last name) must appear on the front of the card.
- The front of the card is considered the side with the electronic contacts.

6 System Security

This section provides details on the Registered Traveler system security including recommendations for Service Provider operations. It is meant to clarify and expand on security-level information referenced in other sections. This section includes a full summary of the RT system chain-of-trust, securing messages between domains, providing a component-level key management, physical security of workstations, and other issues to be covered by policy statements.

Please note, this document outlines a set of security measures that are necessary for ensuring security and privacy of data in the context of interoperability. However, it is very important that Service Providers also implement the necessary security policies and controls outlined in the TSA RT Security, Privacy and Compliance Standards document.

The fundamental requirements of RT system security are to keep data private, intact, available as needed and only transmitted to systems with a 'need to know'. Therefore, all sensitive data shall be encrypted at the initial collection point and remain encrypted throughout the process (except where data processing is required). All data transfers between systems shall require authentication of participants. Data verification shall rely on digital signatures for authenticity and integrity. Together, these overarching fundamental principles combined with security policy requirements form the foundation for the chain-of-trust. Building on this foundation are the RT security services that shall protect stored, processed, or transmitted data through one or a combination of the following capabilities: confidentiality, integrity, authentication, non-repudiation, accountability, and availability.

The Registered Traveler program avoids using a Public Key Infrastructure (PKI) at the member-level due to implementation costs, certificate management complexity, and the time frame needed to draft and approve a security policy. Avoiding the assignment of certificates to individual users for the purpose of identification contributes to significant cost savings to SPs. Personal identification and the protection of sensitive data are achievable on the smart card using biometric matching technologies and shared symmetric-key authentication.

Biometric identification is integral to the Registered Traveler program. A member must biometrically match against smart card data to reap the benefits of the program. In similar programs, user consent and authentication for accessing this data is supplied through a PIN. However, the business model of the Registered Traveler program shows that a PIN is not feasible for the traveling public. Using alternative methods of demonstrating identity is necessary for the purpose of RT. Prior to enabling an RT credential, VPs are required to acknowledge cardholder consent which is implied when the user presents their card to the station reader. The use of contact-only cards requires the user to slide their card into a reader slot, thus making it obvious that data is being read from the card. Contactless smart cards are not currently supported so the mechanism for obtaining user consent for such cards is yet to be defined. User identification is achieved via a 1:1 biometric matching algorithm, and authentication for accessing this biometric data is accomplished using mutual authentication.

Protecting sensitive data is also an integral part of the Registered Traveler program such that members can be highly confident that their biographic and biometric data stored on the smart card are released only to approved and authenticated systems. Use of the RT applet data is restricted to TSA-approved applications (SPs may use additional applets on the card for other applications). Mutual authentication using diversified symmetric keys accessed using secure key management devices provides a mechanism for communication between smart card and verification station to ensure both parties authenticate each other, as explained in Section 5.6, Card/Verification Station Authentication and Key Management. Using

this level of protection along with a contact interface, encryption of sensitive data held inside or transmitted by the smart card (after mutual authentication) is not necessary. To help prevent compromise, key management devices are also restricted to TSA-approved environments. And, while a compromise of the master key used for diversified key generation may allow the card data to be read, mechanisms are available to replace cards that use the key. Old cards would have their payloads revoked and those in the possession of the RT Participant (which remain private) are recalled and destroyed. Then replacement cards may be issued with a new biometric payload and a new master key following a rollover process such that protection of the data is retained.

6.1 Chain-of-Trust

The goal of the Registered Traveler program as an end-to-end interoperable system is to maintain a strict chain-of-trust from enrollment through verification. This will be accomplished by a trust model that ensures data integrity, sensitive data confidentiality, and system authentication within and across domains. A scaled version of a PKI, symmetric encryption and mutual authentication techniques, and policy statements for ensuring conformance will drive how the model satisfies these requirements.

The chain-of-trust between domains is quintessential to the interoperable security model. Service Providers must be able to exchange information with the CIMS such that the end-points are mutually authenticated, message data cannot be altered, and sensitive data is not disclosed to unintended receivers. This chain begins with a centralized Certification Authority (CA) responsible for issuing X.509 V.3 certificates to the CIMS and SPs with a policy that is applicable only to the RT business domain. The TSA will designate the agent that will operate the CA for the RT program. Each SP in the RT domain is assigned a certificate for messaging authentication. All certificates conform to a single security policy such that their purpose is to authenticate the originator, ensure data integrity, and provide non-repudiation. Roles and privileges are controlled by the system and not through the certificates themselves. For example, if an SP is no longer allowed to send submissions to the CIMS, revoking their messaging certificate is not necessary. The CIMS maintains a list of authorized SPs and is responsible for identifying the provider and denying any enrollment sent by them. This is managed separately from the validity of the certificate itself.

An EP and the CIMS shall also use asymmetric keys to sign smart card data. For both, a separate certificate is issued for this purpose. An EP may have physical separation between the storage facility domain and the card creation process. Plus, there is a logical separation of signing data at rest and data in motion for messaging. The compromise of a key or an expired certificate in one usage should not affect the security functions of the other.

Corresponding to the centralized CA, a centralized method of generating and distributing symmetric keys that are used between systems for smart card authentication is required. When used at a publicly available verification station, these keys shall be stored on a dedicated, tamper-evident hardware security module (HSM) that meets FIPS-140 level 2 (or higher) certification with mutual authentication for protecting access to the key. Figure 6-1 shows the centralized nature of the CA and the Master Key Store which holds the master key. The CIMS also centrally generates diversified card keys for use by the EP in creating cards. The management of these keys and certificates is described in Section 6.3, Key Management.

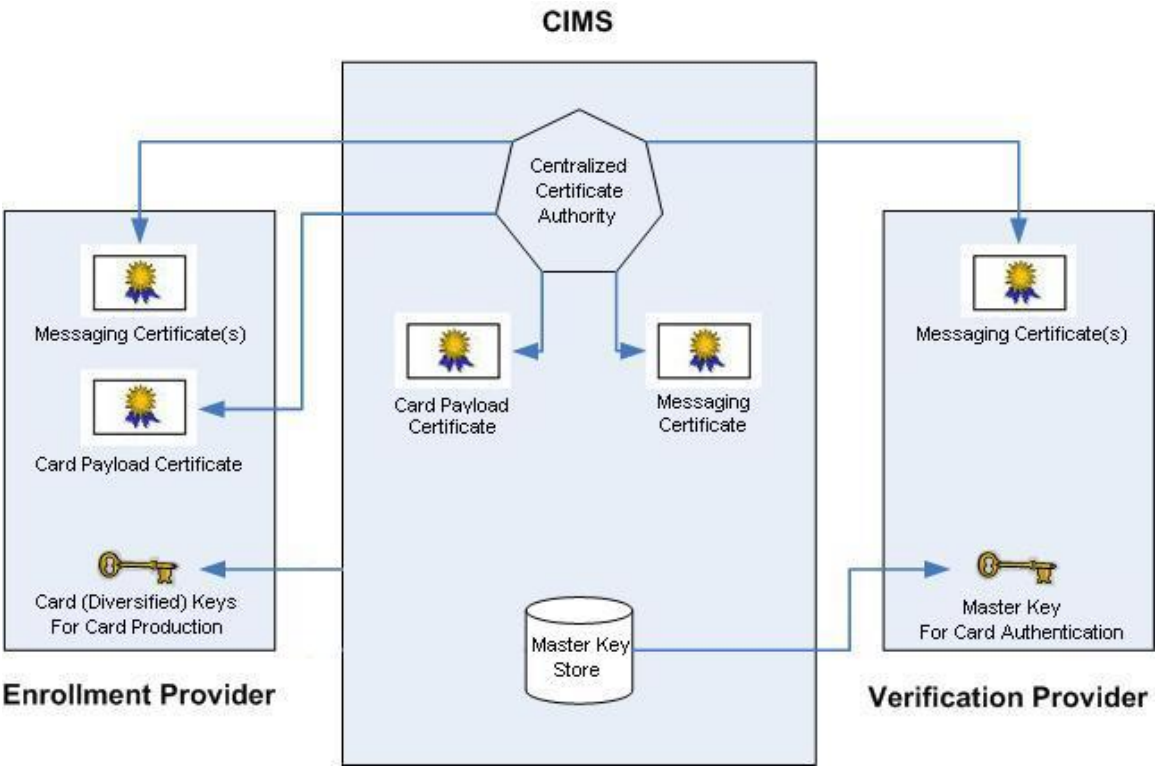


Figure 6-1. Certificate Authority and Master Key Store

Lastly, an internal chain-of-trust per SP shall be required per TSA guidelines to ensure traceability and authenticity of enrollment data and Card Revocation List (CRL) distribution. The following sections detail how each major piece of the RT system contributes to the chain from enrollment to card lifecycle.

6.1.1 Service Provider to CIMS Domain Boundary

Messages from an SP to the CIMS shall be signed by the SP and verified by the CIMS using the message authentication certificate issued by the centralized CA. This certificate policy applies to both EPs and VPs to ensure integrity and non-repudiation of the message, and authentication of the sender. The VP is required to uniquely authenticate itself to obtain a CRL, while an EP shall uniquely authenticate itself for any message (enrollment, revocation, etc.) sent to the CIMS. Sensitive attributes within these messages shall be encrypted as specified in Section 4.2.5, Message Content.

6.1.2 CIMS to Service Provider Domain Boundary

Messages from the CIMS to an SP shall be signed by the CIMS and verified by the SP using a certificate as issued by the centralized CA. This ensures the integrity and non-repudiation of the message as well as the identity of the CIMS. This includes response messages from enrollments, CRL content, and CRL notifications. Sensitive attributes within these messages shall be encrypted as specified in Section 4.2.5, Message Content.

The CIMS shall manage the chain-of-trust from SP enrollment to TSA Security Threat Assessment (STA). Upon successful STA and acknowledgement from the EP, the CIMS shall delete the biographic data for privacy purposes. Upon card re-issuance or de-duplication, the CIMS acquires the biographics from the TSA and re-associates them with the specified RTID. This ensures the previously approved chain-of-trust that was made during the STA process without requiring the CIMS to store all the data.

6.1.3 Card Creation and Authentication

As well as signing communication messages between domains, SPs and the CIMS are responsible for signing data stored in the smart card for the purpose of ensuring a chain-of-trust from card issuance to card usage at a verification station. This includes a digital signature from the smart card Security Object by the CIMS and a digital signature from the smart card RTUID container by the EP, as specified in Sections 5.3.9, ICAO Security Object, and 5.3.2, RTUID Object. The Security Object on the smart card consists of hashes of data elements (using SHA1 hash, see Table 6.1) that exist in the containers. Instead of reading and validating all the data on the card, the verification station can verify the Security Object signature thus authenticating the full payload. The verification station only needs to check the data elements it plans to process to ensure data integrity (no need to check unprocessed elements). The Security Object creates a binding between the vetted biometrics, biographic information, and the Payload ID on the card. Furthermore, the signed RTUID container which houses the Payload ID (SPID/RTID/ADSN and expiration date) binds the card creation process at the EP to that RTUID. This signed data, along with the fact that smartcard objects are read-only and cannot be modified after initial creation, protects crucial data from being altered. Each signature shall be accompanied by a public-key certificate to verify the contents and ensure that the trust chain maps to the issuing CA via the root certificate.

While these digital signatures ensure payload integrity and authentication, device authentication used to protect privacy is achieved by requiring the EP to obtain and use a symmetric card key for each authentication payload. The CIMS generates this key using a diversification technique on the master key. To complete the chain-of-trust, the verification station shall be required to authenticate with smart cards using the mutual authentication scheme as illustrated in Section 5.6.8, Mutual Authentication Transaction with Card, as well as verify signed smart card content through digital signatures. Figure 6-2 shows the certificates and keys for use in determining the chain-of-trust between SPs.

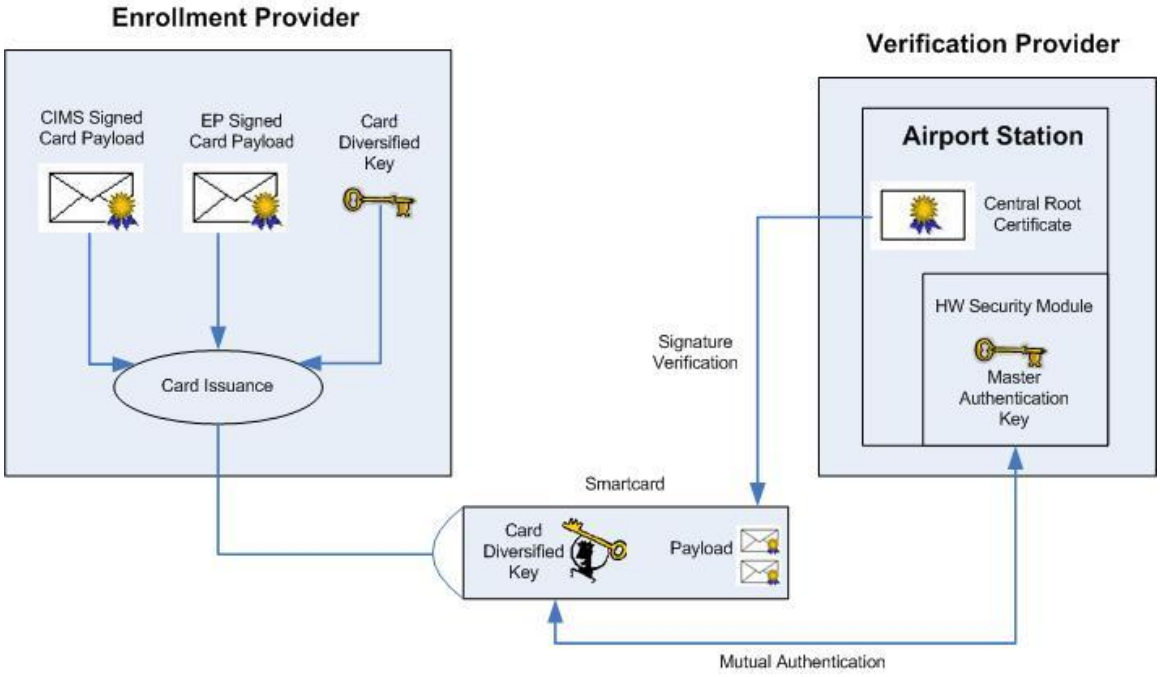


Figure 6-2. Chain-of-Trust from Card Issuance to Card Usage

To ensure the chain-of-trust between card issuer and verification process, the following steps are followed. The user presents their card to the verification station for consent. The verification station connects to the card, reads the Security Object, and verifies the CIMS signature. The EP signature is also checked on the RTUID. If either is not validated, or if either certificate is expired, then the card is rejected. After signature verification, a hash of the Payload ID shall be generated and compared against the hash contained in the Security Object. If the hash does not match, then the card is rejected. The expiration date is checked. If it is less than the current date, then the card is rejected. The SPID/RTID/ADSN is checked against the CRL and if present, then the card is rejected. Next, the mutual authentication process shall take place to unlock biometric and biographic containers. The data can then be read and used as long as its hash matches the associated hash in the Security Object. Thus, the biometric data is used for live identification matching. Passing all these steps ensures the user is a valid member of the RT system by checking the chain-of-trust between systems and the identity of the individual.

6.1.4 Internal Trust

Although the RT program chain-of-trust is meant to define the interoperable security requirements between domains and across all valid smart cards, there exists the need for the trust chain to extend into SP systems. While this is not a mandate for the implementation details of this desired trust chain, it is a declaration that a security infrastructure must exist within the SP domain and be available for proofing by the TSA Security, Privacy and Compliance Process. Details of the internal trust model requirements are outlined in Section 6.5, Security Policies.

The internal chain-of-trust begins with the traceability of the Enrollment Operator for each transaction they create. An RT enrollment workstation shall have the capability to record operator traceability such that each transaction completed by that operator can be tracked back to them. Enrollment Operators shall biometrically authenticate themselves as they complete each enrollment package. Thus, the EP shall perform a 1:1 match prior to forwarding enrollment messages to ensure traceability from enrollment package to Enrollment Operator. An Enrollment Operator identifier shall be recorded by the EP, forwarded to the CIMS, and sent to the TSA for the purpose of discovering trends and identifying the creator of a fraudulent transaction. The link from the identifier to the operator biometric shall be contained at the EP and maintained for the life of the provider as specified in the TSA Security, Privacy and Compliance Process. Note that there is no requirement for distinctly identifying operators with user-level PKI certificates. However, this does not preclude SPs from providing their own non-repudiation methods for this purpose.

Any data sent over a network must be validated to ensure it has not been modified in transit and authenticated to ensure the identity of the sender. Examples of this include enrollment data from a workstation to a central processing server, smart card payload transfer to a card production facility, and CRL data distribution to verification stations. Figure 6-3 shows example linkages within enrollment and verification domains where chain-of-trust shall be maintained.

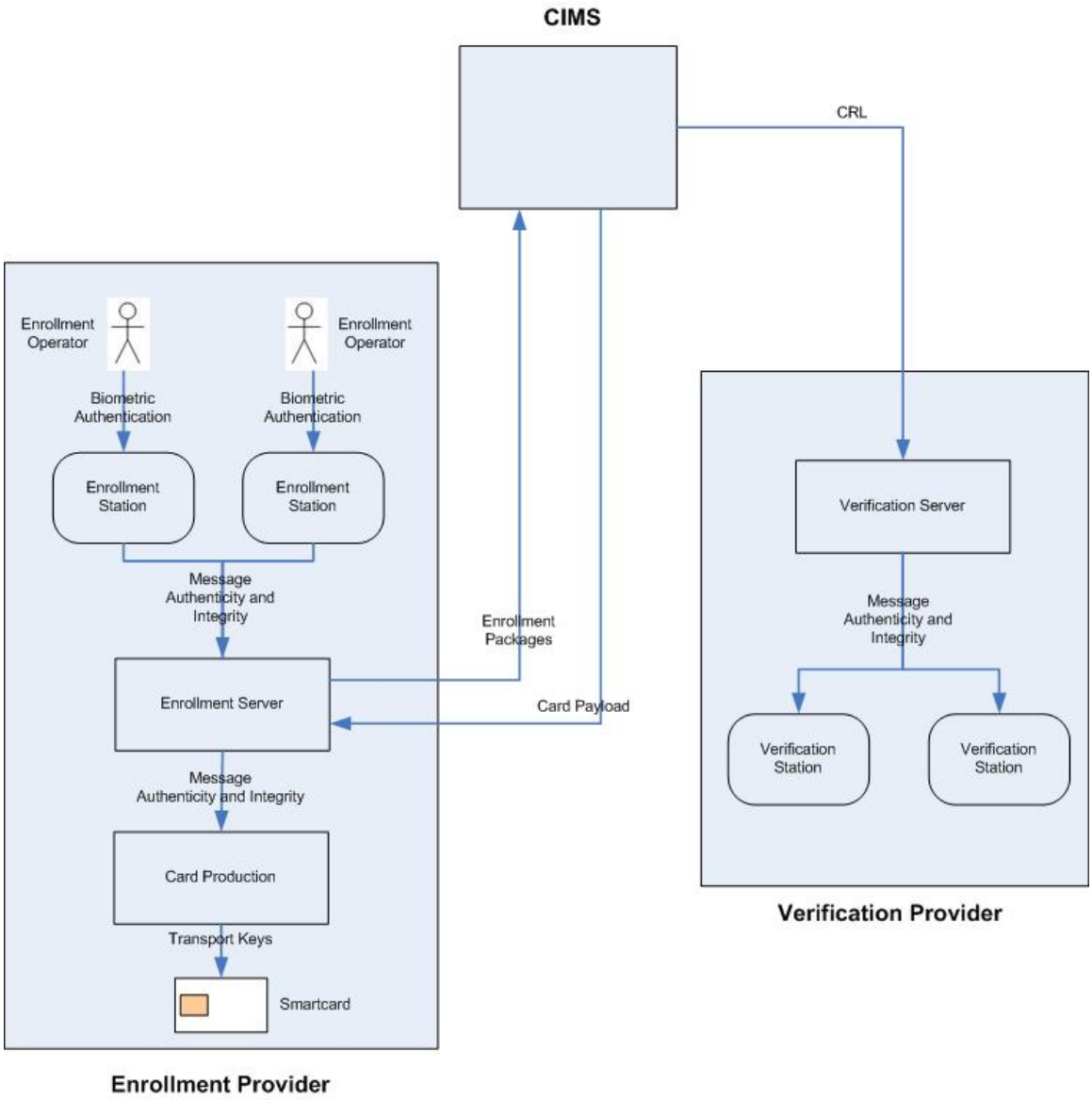


Figure 6-3. Internal Chain-of-Trust Consists of Traceable Operator Enrollments and Authenticated Messages

Smart card manufacturers within the EP domain shall utilize transport keys to maintain security throughout the card creation process. Transport keys provide a mechanism to lock smart cards and protect sensitive data while the smart card is in transit between untrusted parties.

6.2 Message Security

To accomplish the chain-of-trust in system messages between domains, this section defines requirements that detail how certificates and keys are used for confidentiality, integrity, and authenticity. Protecting message data across domains in the RT system follows a two-fold security model such that sensitive data is encrypted at rest, and the entire message (including non-sensitive data) is encrypted during transit through the use of secure communications standards.

Securing the data at rest, prior to sending the message, is accomplished by using a generated symmetric session key to encrypt sensitive fields. The sender then uses the receiver's public key to encrypt the session key and attaches it to the message. The receiver uses their private key to decrypt and discover the session key. The receiver is now able to decrypt applicable contents with the session key. Section 4.2.5, Message Content, defines the structure of a message including which fields are protected, the location of encrypted contents, and the location of the enciphered session key using the XML Encryption standard.

Securing data during transit is accomplished by a transport layer security mechanism for an added layer of privacy and data integrity. SSL 3.0 or TLS 1.0 shall be used to secure communications over the public networks connecting RT domain components. This is accomplished by connecting via HTTPS (secure hypertext protocol) to an application on the receiver end. HTTPS is a combination of normal HTTP interaction over an encrypted SSL or TLS transport mechanism. This ensures reasonable protection from eavesdroppers and man-in-the-middle attacks. The web server has a public-key certificate as generated by the centralized CA for the purpose of messaging so clients can verify the certificate chain for authenticated communications.

To ensure message authenticity, integrity, and non-repudiation, messages passed between domains shall be accompanied by a digital signature. The sender shall generate a signature for the receiver to verify following the standards outlined in Section 4.2.3, Message Header, which explains the use of the XML Signature standard. Public-key certificates required to validate the signature are distributed separate from the message. These certificates are generated for the message sender by the centralized CA for the purpose of messaging as specified in Section 6.1, Chain-of-Trust. Trust is determined by verifying that the certificate is signed with the CA root certificate that shall exist in the receivers trust store. Section 6.3.1, Public Key Management, summarizes the distribution of these certificates.

6.3 Key Management

A security solution must support secure key management methods for key creation, distribution, verification, storage, revocation, and rotation. Each stored key in the RT system must be associated with either an authorized SP or the CIMS. Key management shall provide for the following:

- Secure support for the accepted types of keys and certificates needed for encrypting data stored in online and offline media, and data in transmission.
- An auditable means for systems to register, authenticate, retrieve, exchange, renew, and retire keys.
- Minimizing the number and variety of keys and certificates cumulatively used and supported for security services.
- Secure storage of keys and certificates across SPs.
- Backup and restore of keys and certificates with regard to backup and restore of encrypted data.
- Automated certificate distribution and revocation.

6.3.1 Public Key Management

6.3.1.1 Certificate Generation and Distribution

All certificates generated by the centralized CA are issued upon the accreditation of a SP to conduct business within the RT program. Certificate requests will originate from the respective SPs (enrollment or verification) who are responsible for generating their own public/private key pairs. The CA is responsible for manually assuring the identity of the requestor to avoid issuing certificates to incorrect sources. Once the association between the SP and the public key contained in the certificate request is verified, the CA will issue the appropriate certificates to the requesting entity. This is also a manual process such as an e-mail with the newly created certificate attached, or simply a notification that the certificate is available for public fetching. Each certificate must be restricted in assignment to a particular host within an SP environment to avoid the need to share a private key across systems. This means one messaging certificate shall be assigned to every RT domain component messaging endpoint. If an EP and VP share the same host, then only one certificate is needed for messaging purposes. Service Providers shall protect their private keys from disclosure at all times.

The CA digitally signs each certificate that it issues with its private key to provide the means for establishing authenticity and integrity of the certificate. Because certificates used for signing smart card payload are included in the smart card payload, they do not need to be distributed to all VPs. Verification stations shall have access to the Root CA certificate to validate the trust chain of signed card payload.

For trusting messages, SPs and the CIMS need access to the sender's public-key certificate and the Root CA certificate. These certificates are made available and shall be manually verified to avoid the risk of a man-in-the-middle attack. The CIMS shall distribute the Root CA certificate and the SP shall manually determine its validity (for example, by phoning the CA Operator and verifying the certificate checksum). Similarly, the CIMS and SPs need to exchange their messaging public-key certificates since they are not included in the message content. The system then installs both certificates into a trusted CA store for validating communications.

6.3.1.2 Certificate Revocation and Expiration

It is the responsibility of the SPs and CIMS to adequately protect all signing keys. In the event of a compromise to a key used for messaging purposes, the SP or the CIMS shall notify the CA and request a new certificate. The CA shall revoke the old certificate. Any communications using a revoked certificate shall be rejected and mitigated in a manual fashion. Upon manual notification of a revoked certificate, a system shall remove it from their trusted certificate store such that future communications using that certificate are invalidated. All future communications shall use the newly generated certificate. Follow-up investigation and response for key compromise will be addressed by the TSA Security, Privacy and Compliance Process.

In the event of a compromise to a key used for signing card payload, the EP shall notify the CIMS and request a new certificate. The EP shall take all necessary action to determine and mitigate the risk associated with the key compromise. All cards that were created using the key must be revoked to ensure that only truly authenticated payloads exist within the system. The new certificate shall be used to sign all post-compromise card payload data. Using this security policy, VPs need not check the revocation status of a certificate contained on the smart card. This is because only authenticated cards exist using the valid, pre-compromised certificate, all other cards (potentially using the compromised key) would be marked as revoked. The sole purpose of the certificate is to verify the integrity and authenticity

of smart card data. The validity of the smart card data is determined by other means such as the CRL, the on-card expiration date, and the cardholder biometrics.

Certificate expiration is dependent upon use. Messaging certificates will have an expiration at the discretion of the central CA. An expired messaging certificate shall be handled in the same manner as a revoked messaging certificate. The message certificate shall be replaced prior to expiration such that future communications use the new certificate and signatures using the old (expired) certificate can be flagged as invalid. Smart card signing certificates shall be valid for six (6) years and issued annually such that a valid smart card shall never contain an expired certificate. Since the smart card has a maximum valid timeframe of five years, the annual refresh of the payload signing certificate ensures this. In the case that a certificate is presented by the smart card is expired, the transaction shall be rejected.

6.3.2 Master Key Management

6.3.2.1 Master Symmetric Key Generation and Distribution

The RT applet and the verification station utilize a Mutual Authentication (MA) protocol to verify that the other is a valid entity within the RT program. MA is implemented via a symmetric key encryption algorithm, utilizing a key diversification technique to protect the master key (KM).

A certified EP will issue cards with the RT applet containing a card key (KC) derived from the KM. This derivation process is the result of algorithmically combining the KM with static, yet unique, card data to result in the KC, a key value whose construct cannot be reversed to determine the original KM. The rationale for using a key derivation methodology is to lessen the impact should a single KC be compromised. Gaining knowledge of one KC does not reveal the KC of other cards, nor will it expose the KM. An EP does not need access to the KM since each authentication payload generated by the CIMS has an accompanying KC for on-card storage and usage.

The KM is generated by the CIMS and distributed to all certified VP stations using HSMs with FIPS-140 level 2 (or higher) certification. These modules shall never release the value of the KM, but instead use it to perform mutual authentication operations. Access to the KM functions stored in the HSM is further protected using layered security. First, the HSMs are not authorized for use outside TSA-approved environments thus limiting the accessibility. Next, to unlock the device (prior to using its cryptographic features to calculate a KC) requires direct mutual authentication with a HSM activation smart card used by station operators. This card is distributed by the CIMS in the same manner as the HSMs. Activation of a HSM is limited to pre-configured cards only. Each HSM contains logic to interact with certain activation cards, and the keys to do so are kept in the physical devices.

In the case an HSM or activation card is separated from the station, it shall be rendered inoperable. The device's access state shall be reset upon loss of power such that it will need to be reestablished if plugged back in. The keys cannot be read from the HSM, and the HSM is inactive at power-up until it receives authorization from the activation card kept separate from the station. Thus, even the compromise of the HSM and/or activation card is not necessarily a compromise of the KM.

Distribution of HSMs is currently planned as a manual process where VP personnel shall transfer the modules from the CIMS site to verification station. Every time a new KM is issued, a new module shall be updated or distributed, requiring transportation of the module to the CIMS site.

Each distributed KM will have a version number associated with it, enabling SPs to keep track of which KM should be used in an MA operation. The RTUID specifies the KM version used by the particular card which is provided to the HSM for it to select the applicable KM. A hardware security module is expected

to handle at least 20 active, versioned KMs at any one time. This shall allow for sufficient KM escrow which may be necessary to communicate with all valid cards due to KM rollover as explained below.

6.3.2.2 Master Symmetric Key Rollover

From time to time, the KM will experience a rollover, meaning the production KM will be replaced with a new KM. This will occur every two years or for every 1 million cards issued, whichever is greater. This new KM will reflect an updated version number. KM rollover is intended to lessen the impact of the unlikely event of a KM disclosure. Recall that a KM is stored in a hardware security module. If a KM is in fact disclosed, then all cards issued with that KM would be affected. The periodic rollover reduces the potential number of affected cards. Using this rollover method requires multiple KMs to be managed as existing valid cards may use a previous KM version.

6.3.2.3 Master Symmetric Key Compromise Mitigation

In the RT system, the KC is used solely for MA of the station and the applet. This operation provides an additional layer of security for the protection of the information stored on the card. In the unlikely circumstance of a KM compromise, the RT system is, in itself, not compromised to the extent that unqualified persons would be able to breach the RT security. In fact, the only exposure would be that RT applet data could potentially be read by unauthorized entities. It is also important to note that RT data does not specifically contain any personally identifiable information (Social Security Number, address, etc.) although this is partially at the discretion of the EP, and that any biometric data (fingerprints and iris) stored in a template format cannot be reconstructed into the original input images. A KM compromise only strips away one layer of a multi-layered security envelope.

It is the responsibility of the CIMS and VPs with access to the KM to protect it at all times. A key compromise is defined as the loss of a HSM and any activation card that applies to it, thus a level of collusion is assumed to exist whereby the KM may be accessed. In the event of a key compromise, the VP shall notify the CIMS immediately. The CIMS shall perform an immediate KM rollover and notify all SPs. All checkpoint verification stations shall be updated with the new KM version. The old KM version will also be maintained for support of existing cards until they are replaced over a period of time (at the participant's, EP's, and TSA's discretion). Depending on the level of perceived KM exposure, RT Participants holding cards issued under the old KM may need notification that their card is potentially at risk of being accessed without their consent if lost or stolen. To mitigate the risk, the cards can be replaced. All new RT smart cards shall be issued using the newly created and distributed KM. In the event a KM rollover is eminent, the rollover schedule is simply accelerated. Follow-up investigation and response for key compromise will be addressed by the TSA Security, Privacy, and Compliance Process which reserves the right to request a full card replacement if necessary, across all Service Providers.

Note that because of the multi-layered security features, there are methods of addressing lost or stolen HSMs and activation cards such that an accidental key compromise can be avoided. The CIMS may replace HSMs and HSM activation cards in the following cases and the RT system may continue to operate as normal with the assumption that the KM has not been compromised: 1) if an HSM is lost or stolen, and if all activation cards that are able to authenticate to the HSM can be accounted for, and 2) if an HSM activation card is lost or stolen, and the HSM is still present.

6.4 Physical and Logical Station Security

Although enrollment and verification stations will not retain biographical or biometric data, physical and logical security of the station equipment such as fingerprint readers, iris imagers, cameras, computer

screens, and computer software is required. The security of these stations shall consist of physical lockdown requirements, logical restrictions to sensitive data, and an auditable servicing process.

Enrollment and verification stations are to be deployed within airport terminals throughout the US, and potentially other regions. Since the stations are deployed in a public space in the airport, it is an assumption of the security model that a station is at a risk of compromise. Many of the security control measures described here are explicitly designed to mitigate this assumed vulnerability. The station design shall prevent unauthorized users from obtaining access to hardware and software that may be used to fraudulently access the RT domain and any sensitive data within it.

The station shall be physically configured in a robust manner to make it an undesirable target for system penetration. Any CPU(s), data storage devices, or communications equipment shall be secured in a locked unit, accessible only by authorized maintenance personnel upon determination of employment and permissions. The locking mechanism is tamper-resistant but not tamper-proof. In the event an electronic mechanism is utilized, it shall be constructed so as to remain in locked mode in the event operating power has been removed from the station. Only the monitor(s), biometric readers, document scanners, and other human interface devices are accessible by station operators. Operators are responsible for daily monitoring of the physical status of the stations and immediate reporting to their supervisor of damage, theft, or other tampering. An approved auditing procedure will be implemented to record access to the secure station enclosure.

Station operators with access to sensitive information shall have logical access accounts, managed by the Operating System, that are configured with the appropriate privileges. Access to station Operating System by non-privileged users is restricted to maintain the integrity of the system. The station Operating System, and thus the software and hardware controlled by it, shall be locked from unauthorized access when the station is not in use. Only authorized personnel may unlock the workstation using approved logical access controls. There may be privileged user accounts, such as administrator, which are available to the users that require an unrestricted access level. Enrollment Operator accounts will be configured to have access to only the minimum system resources required to perform an enrollment. Enrollment Operator accounts will not have administrator privileges.

Enrollment and verification stations shall be restricted from self-activating. That is, the station shall have checks in place, prior to starting full operations, to obtain user access credentials. For verification stations, access to the HSM shall be established prior to operation and never be automated. Repeated unsuccessful attempts at accessing the module or station itself shall render them inoperable until reset by an administrator. The HSM itself shall also be restricted to TSA-approved environments (such as the airports). If the EP wishes to support external usage of the RT card (through another applet or the reserved SP data object), other access means must be implemented.

The information at RT enrollment and verification stations must be protected against compromise through encryption technologies described in Section 6.5.1, Algorithms and Key Lengths. Therefore, in the event of unauthorized access to station hardware or software, any sensitive data will be protected.

Service Providers are required to keep documented records/service logs of authorized station personnel servicing the RT stations. Any attempt at updating enrollment or verification station hardware and software shall record an operator identifier and the action performed. The TSA Security, Privacy and Compliance Process shall approve a Configuration Management process for each RT domain component for the purpose of ensuring that any hardware or software change is handled appropriately and that any security infrastructure change is approved and tested for conformance as necessary. The process will also determine if the change warrants a need for re-testing conformance.

The audit trail supports accountability by providing a trace of user actions. Audit trails are designed and implemented to record appropriate information that can assist in intrusion detection. Audit trails include sufficient information to establish what events occurred and who (or what) caused them. Verification events are also audited but do not have to be explicitly recorded against an operator. More information on verification event recording is specified in Section 4.5, RT Participant Verification. Access to audit logs is strictly enforced. Only system administrators have the appropriate permission to review audit logs.

6.5 Security Policies

The need for security policy statements is required to cover the business rules for securing the RT system and its domain components. These rules and regulations are designed for SPs to follow and be able to achieve certification through the TSA Security, Privacy and Compliance Process. The effective strength of RT cryptosystems and the coverage of operational policy statements will ultimately determine the degree of confidentiality, integrity, non-repudiation, authentication, accountability, and availability that an RT system component contains and shall maintain throughout the life of the RT program.

6.5.1 Algorithms and Key Lengths

The strength of encryption algorithms depends on the algorithm's design, key lengths, and the controls for key and certificate implementation and support. The following table outlines the required algorithms for protecting data that is required to be secured at rest or in-transit, as specified throughout this technical specification regarding messaging between RT domain components, smart card digital signatures, and RT applet mutual authentication. Service Providers must adhere to the CIMS Service Level Agreement which may take precedence over the following requirements.

Medium	Description	Security Provided	Standard
Message	Data is at rest in a message body.	Privacy	AES
Network (Client-Server)	Data is in motion (transmitted) between machines.	Integrity, Privacy, Server Authentication	SSL 3.0 or TLS 1.0 using RSA 1024-bit X.509 certificates AES for symmetric ciphering SHA-1 for hashing
		Integrity, Non-repudiation, Client Authentication	RSA 1024 bit X.509 certificates for digital signatures with SHA-1 for hashing
Smartcard or HSM	Data is exchanged between devices to express knowledge of a shared secret.	Mutual Authentication	128-bit 2 Key Triple DES-ECB

Table 6-1. Interoperability Algorithmic Requirements

Requirements exist throughout this technical specification, including Section 6.5.4, Operational Policy, for securing data within an RT component domain (not part of the interoperable domain crossings). While

the method for doing so is at the discretion of the system owner (in conjunction with the TSA), the following table shows the minimum algorithm requirements to meet.

Medium	Description	Security Provided	Standard
File	Data is at rest as a file on a file system.	Privacy	AES
Message	Data is at rest in a message body.		
Database	Data is at rest in a database column (field).		
Network (Client-Server)	Data is in motion (transmitted) between machines.	Integrity, Privacy, Server Authentication	SSL 3.0 or TLS 1.0 using RSA 1024-bit or DSA 1024-bit X.509 certificates AES for symmetric ciphering SHA-1 or MD5 for hashing
		Integrity, Non-repudiation, Client Authentication	RSA 1024-bit or DSA 1024-bit X.509 certificates for digital signatures with SHA-1 for hashing

Table 6-2. Minimum Standards for Service Provider Algorithms

With the continual progress of computing technologies, there exists the need to constantly certify the effectiveness of a crypto-system. Therefore, the security key length requirements expressed here shall be reviewed annually and upgraded as technology allows. This may require RT domain components to agree on new or updated standards for future use. According to SP-800-78, certain algorithms and key sizes specified here have a defined time period for use. It is recommended that software and hardware systems within the RT domain are built with expansion capability for easier transition in the future rather than being forced to update and modify systems later. For example, it is specified that after 2010, 2 Key Triple DES shall be replaced by 3 Key Triple DES. This may affect the design of hardware security modules and message sizes throughout the RT infrastructure.

6.5.2 Sensitive Information Protection

Considering the significance of the personal information provided by RT Applicants that will be maintained by SPs and CIMS databases, it is essential to provide security measures within each environment to serve as best-practices for handling sensitive information. The TSA Security, Privacy and Compliance Process shall further define and validate specific requirements for protecting information within an RT domain component and for employee screening procedures.

Each person that is responsible for handling sensitive information must pass a screening process commensurate with the level of access required. Persons with access to sensitive information within a domain shall have logical access accounts that are configured based on the job function the user performs on the program with the appropriate privileges. Access to systems by non-privileged users must

be restricted to maintain the integrity and configuration control of the system. There may be privileged user accounts, such as administrator, which are limited to the users that require an unrestricted access level. All logical access accounts shall require authentication, such as password protection, for identity verification.

Sensitive data fields shall be protected to avoid accidental dissemination. For example, account numbers or Social Security Numbers can be partially masked as an added layer of securing the data, even from approved system users. Access to detailed, complete personal information should be on a need-to-know basis, controlled through access list and only available to supervisors or appropriately vetted persons. Access to the full information set shall be traceable by audit log.

Computer rooms and/or equipment rooms that house sensitive data internal to an RT domain component shall be secured 24 hours a day, 7 days a week. Equipment used to process, store, transmit, and receive RT cardholder data shall be considered protected resources. Further physical security requirements for an RT station are specified in Section 6.4, Physical and Logical Station Security. The following guidelines are recommendations for all protected resources:

- All data centers are controlled by authorized personnel.
- All servers, switches, and routers are located in a computer room that is locked using a card-key or combination lock system for entry.
- All cables are installed to provide shelter from tampering, unauthorized access, or other risk.
- Penetration from ceiling or floor into the computer room should be prevented.
- All closed-circuit television equipment is enclosed and safe from tampering.
- All modems are located in a restricted location.
- All printers are located in a restricted location.
- Printed output of RT Cardholder data is processed in a restricted location.
- All workstations and display monitors are located in a way to prevent reading sensitive RT cardholder information.

6.5.3 Public Network Recommendations

Using vulnerabilities associated with Internet protocols and website application, today's hackers can develop extremely sophisticated and easy-to-use tools to override most security and employ web application specific attacks, data destruction, and exploits such as URL tampering, database injections, buffer overflows, website defacements, and cookie poisoning. The potential costs of exposure, destruction, or modification of key data, such as social security number, or date of birth, are tremendous. It is recommended that publicly accessible networks employ firewalls to restrict communications (ports, services, hosts, and traffic) as specified by the specific RT domain's security policy. Intrusion Detection Sensors are recommended to detect malicious and suspicious activity such as port scans, denial of service attacks, or other intrusion attempts. Segregation of external and internal components is recommended to limit the amount of exposed data.

6.5.4 Operational Policy

The TSA Security, Privacy and Compliance Process, which defines security infrastructure requirements, is responsible for proofing the security infrastructure of an SP. An SP is responsible for defining a

security policy against which to be measured during this process. The following are operational security requirements that are to be followed in additional to the TSA Security, Privacy and Compliance Process. As specified, these requirements extend to all RT domain systems, including the CIMS.

- The information within or between an RT domain component shall be protected from unauthorized release or change. Any sensitive data stored on a station or in a system shall be protected in the event the storage is exposed to unauthorized parties. Any data stored within any RT domain component for the purpose of transmission shall be protected from reading until it is transferred to its intended destination.
- If a verification station is unable to update the CRL to the latest version as expressed by the CIMS in a 24-hour period, the station shall be restricted from operations until the list is updated. This should be accomplished automatically by the station and does not require an operator to take it offline. This may occur via online access or some offline mechanism such as USB file transfer.
- Upon notification from CIMS of exceptional operating conditions (i.e., an unplanned outage) an override for the CRL refresh process may be instated. When the CIMS cannot be accessed, verification operations can continue as normal until notified by the CIMS to do otherwise. The CIMS shall notify VPs to cease operations if TSA revocations are identified during the outage. Verification stations shall be updated as soon as the CIMS communication is re-established if they are outside of the 24-hour update period.
- An enrollment station shall not store personal data of the enrollee beyond successful transmission to the EP storage facility. A verification station shall not store, nor transmit to the VP storage facility, any personal identification data, including the RTID, during and beyond a verification transaction event. This event is defined as the moment of user consent to the moment of successful/unsuccessful smart card validation. To support verification events, a VID is provided for recording. As stated in Section 2.4.3, RT Participant Verification, there are exceptional circumstances where the RTID may be retained and reported, specifically when a credential is presented to the verification station that exists on the CRL as being revoked by the TSA.
- All RT systems shall be kept reasonably up-to-date with Operating System patches. A reasonable time-frame shall be defined in the TSA Security, Privacy and Compliance Process.

7 Conformance Testing within RT

Conformance testing is one of the final stages in the process of introducing a new EP or VP into the interoperable RT program. The purpose of conformance testing is to officially certify a SP's technical and procedural ability to comply with all operational and policy requirements outlined in this document. Achieving conformance certification demonstrates that the SP is fully technically qualified to begin operations.

This section defines the means of verification for RT program interoperability. To achieve system conformance, the following performance measures must be confirmed:

- System interoperability
- Quality of service
- Service levels
- Compliance with common policies and procedures.

This section outlines high level test cases, testing procedures, and the testing environment that will be used to verify that these performance measures are achieved by all participating EPs and VPs.

Detailed conformance information can be found in the *RTIC Conformance Testing Test Plan/Procedures* published separately. Additionally, service providers must meet the requirements of the *TSA Registered Traveler Security, Privacy, and Compliance Standards for Sponsoring Entities and Service Providers*.

7.1 RT Conformance Lab

The RT Conformance Lab plays a central role in both establishing initial interoperability and maintaining interoperability across multiple service providers. The RT Conformance Lab shall house provider platforms and will perform required tests with the active participation of the interested EPs or VPs and the CIMS. The RT Conformance Lab shall establish electronic interfaces for messaging exchange with the CIMS, a secure location to house various VP implementations, a limited number of test cards for each participant, and support preliminary quality testing of the SP's solutions.

All deployed and active versions and configurations of the verification station will be resident at the RT Conformance Lab. The VP will supply all proper configuration instructions and will supply all operating instructions. The SP is responsible for providing all appropriate licenses, all hardware and all software components in an operational state of readiness. To protect the integrity of the RT Conformance Lab, at no time will a VP representative have direct access to the lab without escort. The RT Conformance Lab will implement and enforce policies to ensure the integrity of the lab environment. The RT Conformance Lab shall verify the minimal levels of conformance as specified by this document and may support additional testing to verify higher levels of performance. Additionally, the RT Conformance Lab may modify the details of any testing procedure, subject to TSA approval.

7.2 Critical Tests

The following processes and procedures are critical for the RT Program and will be minimal requirements for interoperability conformance:

- SPs must conform to the specifications for enrollment submission.
- SPs must generate card content that includes correctly formed authentication data received from the CIMS and other data.

- SPs must implement a RT Participant verification process that includes recorded metrics and excludes disallowed data.
- SPs must demonstrate CRL-handling procedures that include the automated cessation of verification station operations if the CRL has aged beyond required parameters.

Conformance testing is defined as follows.

7.2.1 Enrollment Provider Messaging

To test the enrollment submission process, the lab's CIMS will provide the EP with temporary security credentials that will be outside the normal chain-of-trust and will not be used within the production environment. The electronic transport from EP to this CIMS will function as defined in Section 4.2, Communication Architecture, but will connect to a CIMS conformance testing environment rather than the production system.

7.2.2 Card Conformance Testing

The RT Conformance Lab will verify the interoperability of every card configuration that an EP issues. Card conformance testing will take place when a new EP applies to join the RT program, or if there is a change in an existing EP's card platform or card issuance process.

To facilitate repeated and similar testing across all SPs, the CIMS will have pre-defined payloads with test biometric data.

Sample RT cards that pass the card conformance tests will be retained by the RT Conformance Lab to facilitate further testing.

7.2.3 RT Participant Verification Testing

These test cases will ensure that a valid end-user experience is achieved across all currently existing verification stations. This test will ensure system interoperability, biometric functionality, and a consistent end-user experience.

The test will be performed by the RT Conformance Lab personnel and will include a set of standard RT verification scenarios, as well as tests of border conditions. The VP will supply active versions and configurations of the verification station.

Biometric functionality may be tested by the RT Conformance Lab using offline analysis techniques against a pre-compiled and known data set. VPs may be required to provide the biometric verification software separate from the verification station for this purpose.

7.2.4 CRL Management Testing

The objective of this conformance test set is to ensure a standardized and rigorous means of ensuring a VP conforms to the requirements for handling CRLs and entities on CRLs.

During this test suite, the lab's CIMS will revoke Service Providers, RT Participants, and RT Cards. These revocations will appear to come from Service Providers and the TSA.

The RT Conformance Lab will also validate that the verification stations go offline if the CRL has not been updated in the time period specified by the TSA requirements.

7.3 Ongoing Conformance Verification

Methods for managing ongoing conformance verification shall be determined between the TSA, RT Conformance Lab, and the SPs when the V&V documentation is released.

7.4 Conformance Validation and Conformance Expiration

The conditions under which a conformance validation will expire (e.g., based on time, change in hardware or software components) will be defined by the TSA.