



BJA
Bureau of Justice Assistance
U.S. Department of Justice

Global Reference Architecture

Fingerprint Service (FS) Service Description Document

Version 1.0

April 2012



Global
Information
Sharing Standard

Global Standards

Global's collection of normative standards has been versioned independently and assembled into a package of composable, interoperable solutions specifically supporting an information exchange. The package is known as the Global Standards Package (GSP). GSP solutions are generally technically focused but also may include associated guidelines and operating documents. GSP deliverables include artifacts associated with many of the Global product areas, including but not limited to:

- **Global Reference Architecture (GRA):** Offers guidance on the design, specification, and implementation of services (and related infrastructure) as part of a justice Service-Oriented Architecture (SOA).
- **Global Service Specification Packages (SSPs):** Reference services that serve as the means by which the information needs of a consumer are connected with the information capabilities of an information provider.
- **Global Federated Identity and Privilege Management (GFIPM):** Guidelines and standards for establishing, implementing, and governing federated identity management approaches.
- **Global Privacy Technology Framework:** A framework for automating access control (in particular, privacy) policy as part of information exchange.

For More Information

For more information on the GSP and the Global Standards Council (GSC)—the Global group responsible for developing, maintaining, and sustaining the same—please visit <http://www.it.ojp.gov/gsc>.

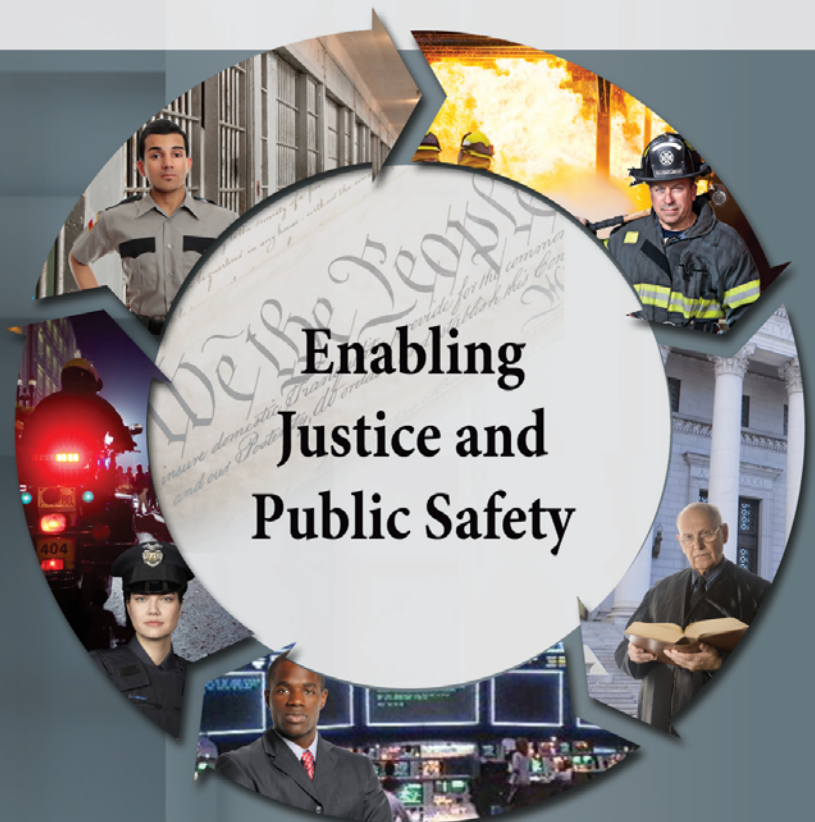


Table of Contents

1.	Document Introduction	1
2.	Service Overview	2
2.1	Purpose	2
2.2	Scope	2
2.3	Capabilities	2
2.4	Real-World Effects	3
2.5	Summary	3
2.6	Description	3
2.7	Security Classification	4
2.8	Service Specification Package Version	4
3.	Business Scenarios	4
3.1	Primary Flow	5
3.2	Alternative Flow	7
4.	Service Interoperability Requirements	11
4.1	Service Assumptions	11
4.2	Service Dependencies	12
4.3	Execution Context	12
4.4	Policies and Contracts	12
4.5	Security	12
4.6	Privacy	12
4.7	Other Requirements	12
5.	Additional Information	13
6.	Information Model	13
7.	Service Model	18
7.1	Data Inputs	18
7.2	Data Outputs	19
7.3	EBTS Message Structure	19
7.4	Data Provenance	20
8.	Behavior Model	20
8.1	Synchronous	20
8.2	Asynchronous	20
8.3	Action Model	21

8.4 Process Model	22
Appendix A—References	25
Appendix B—Glossary	26
Appendix C—Document History	27

1. Document Introduction

In the context of the GRA and Service-Oriented Architecture [SOA] in general, a service is the means by which one partner gains access to one or more capabilities offered by another partner. Capabilities generate real-world effects that can be as simple as sharing information or can involve performing a function as part of a complex process or changing the state of other related processes. Government organizations have numerous capabilities and a multitude of partner organizations, both inside and outside of their traditional communities. There are significant benefits for these organizations to share information and have access to each other's capabilities. Achieving interoperability among these organizations requires alignment of business and technical requirements and capabilities. In addition, it is critical to have a consistent way of specifying these requirements and capabilities and sharing them across organizational boundaries. The GRA was developed to facilitate interoperability and to assist in meeting other key requirements common in a complex government information sharing environment. In order to achieve interoperability, a consistent approach must be defined to identify, describe, and package services and their interactions in many different technical environments, across multiple government lines of business, at all levels of government, and with partner organizations.

The GRA defines a service interface as “the means for interacting with a service.” It includes specific protocols, commands, and information exchange by which actions are initiated on the service. A service interface is what a system designer or implementer (programmer) uses to design or build executable software that interacts with the service. That is, the service interface represents the “how” of the interaction. Since the service interface is the physical manifestation of the service, best practices call for service interfaces which can be described in an open-standard, machine-referenceable format (that is, a format which could be automatically processed by a computer).

A Service Specification is a formal document describing the capabilities made available through the service; the service model that defines the semantics of the service by representing its behavioral model, information model, and interactions; the policies that constrain the use of the service; and the service interfaces which provide a means to interacting with the service. A Service Specification is analogous to the software documentation of an Application Programming Interface [API]. It provides stakeholders with an understanding of the structure of the service and the rules applicable to its implementation. It gives service consumers the information necessary for consuming a particular service and service providers the information necessary for implementing the service in a consistent and interoperable way.

The main components of a Service Specification are the Service Description, one or more Service Interface Descriptions, and the schemas and the samples used to implement and test the service.

A Service Description contains information about all aspects of the service which are not directly tied to the physical implementation of the service; in other words, the service interface. A Service Interface Description is a description of the physical implementation; specifically, the service interface used in a specific implementation of the service.

This document is a Service Description for the Fingerprint (FP) Service.

2. Service Overview

The Fingerprint Service provides positive identification or verification based on the submission of fingerprint information. The service receives one or more fingerprint images and returns a biometrically based response which facilitates the determination of the physical identity of an individual. Identification is defined as the capability to compare a biometric object against a biometric information repository for a biometric match. Verification is defined as the capability to compare a biometric object and a biometrically based identifier against a biometric information repository for a biometric match. In many cases, in addition to the biometric object and the biometrically based identifier, additional information is submitted to the service to allow for search optimization. This information could be personal demographic information or geographic location information.

2.1 Purpose

To provide positive identification or verification of the physical identity of an individual based on biometric information. Events such as an arrest, custodial intake, booking, arrangement, inmate transfer, etc. are typical instances where positive identification or verification is required.

2.2 Scope

The Fingerprint Service provides capabilities which allow identification or verification of the physical identity of an individual through the exchange of fingerprint biometric information and other related information.

Out of Scope: Biometric identification based on other biometrics information, such as iris images; facial images; scars, marks, and tattoo images (SMT); and signature images.

2.3 Capabilities

1. Provide biometrically based identification.
2. Provide biometrically based verification.

2.4 Real-World Effects

1. Law enforcement agencies can use this service as part of the criminal apprehension arrest process.
2. Courts can use this service during the court appearance and bond hearing processes.
3. Federal and state criminal history repositories can use this service during the case creation process and criminal history inquiry response process.
4. Corrections can use this service during the incarceration intake, case file creation, movement, high-value transactions, and release processes.
5. Jails can use this service as part of the booking intake and/or transfer processes.
6. Other governmental agencies can use this service as part of the employment applicants screening and licensing determination processes.
7. Private organizations can use this service in the process of screening applicants for employment or volunteer positions.

2.5 Summary

The Fingerprint Service provides a positive, biometrically based response based on the submission of one or more fingerprint images.

2.6 Description

The service receives one or more fingerprint images and information concerning the inquirer. The service request might also contain additional individual information (e.g., name, sex, date of birth) to assist the service provider in performing a search of its files. In addition, the service messages contain transaction identification information to support the exchange of messages and, more specifically, to relate the response to the inquiry in an asynchronous communication environment.

The service provides either a “no record response” or one or more biometrically based sets of information issued by the responding agency. The response information set includes one or more biometrically based identification numbers and other individual information.¹

¹ A biometrically based identification number is an identification number issued and verified based on biometrical information only (e.g., FBI ID, state ID). The biometrically based identification number may be newly issued based on the current submission.

The service may also provide, as part of the response, other individual information (e.g., name, sex, date of birth, height, weight, driver's license number, social security number). This information is based on prior submissions and inquiries.

Alternatively, the service can provide a yes/no response to indicate a biometrical match between a biometric object and a biometrically based identifier or no match.

This service may be orchestrated together with other services which perform similar fingerprint-based biometric searches or request and receive information related to the individual subject of the identification from other systems based on the biometrically based identification number received as a result of an identification service request.

2.7 Security Classification

The information exchanged by this service is considered Sensitive But Unclassified (SBU). As a result, the service can be assigned a security classification of SBU.

2.8 Service Specification Package Version

This service specification is built based on version 1.0.0 of the Service Specification Package.

3. Business Scenarios

Criminal justice agencies frequently need to determine the physical identity of an individual; this service provides that positive identification or verification. Once the positive identification or verification is obtained, these agencies need additional information to complete the larger process in which they are engaged. For instance, in a bond hearing, a positive identification is required as well as the related criminal history record which is used as part of the bond setting. In the custodial intake process, the biometrically based identification number is used to invoke another service which provides previous incarceration information used to set security classification.

Other governmental agencies require identification or verification for employment applicants screening and licensing determinations. The results of the identification can be used to invoke other services to provide warrant and criminal history information to be used in the determination.

Private organizations may have access to this service for the purpose of screening applicants for employment or volunteer positions. The service response can be used to invoke other services which provide active warrant, registered sex offender, and criminal history information.

In providing the information the inquiring person/agency wants, there are two, not mutually exclusive options:

1. The person/agency uses the response from the Fingerprint Service to perform additional service requests.
2. The Fingerprint Service is part of a composite service built either by the inquiring agency to obtain all the information it needs or by the service provider to provide all of the information it has.

3.1 Primary Flow

- The Consumer System* submits a request for biometrics-based fingerprint identification.
- The Provider System** receives the request.
- The Provider System validates the request and sends a fault message in the case of an invalid request.
- In the case of a valid request, the Provider System performs a fingerprint-based search.
- If a matching record is not found, the Provider System sends a “record not found” message.
- If one or more records are found, the Provider System sends a biometrically based identification response to the Consumer System.
- The Consumer System receives the fault message, “record not found” message, or identification information message.

**The Consumer System is any law enforcement, courts, criminal history, corrections, jail, government agency, etc. system which requires fingerprint identification as part of its designed business process flow.*

***The Provider System is any system which can provide biometrically based identification or verification. In most of the cases, the Provider System is a system which has the capability to store a collection of biometric objects and identifiers. These systems are often referred to as biometric information repositories.*

The following diagram represents the primary process flow in a graphical format.

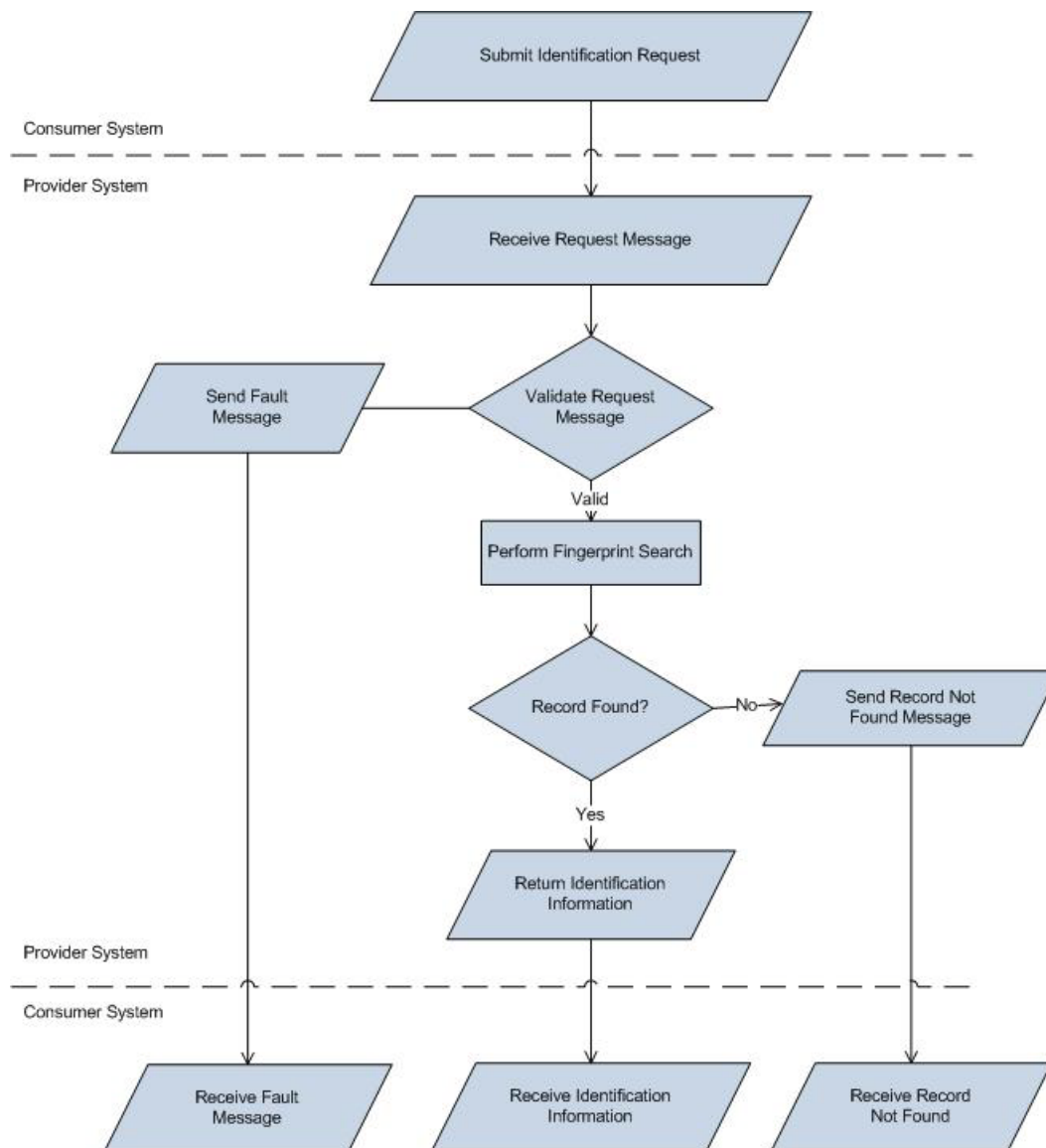


Figure 1: Primary Process Flow Diagram

In certain situations, the Provider System may be required to create a new record in the event that no matching record was found. That requirement is communicated by the Consumer System as a parameter within the request message. In this case, a “record not found” message will not be sent back to the Consumer System. The identification information of the newly created record will be sent instead.

3.2 Alternative Flow

In certain situations (primarily for the purpose of process optimization), it may be necessary to perform fingerprint verification by comparing a biometric object and a biometrically based identifier and providing a yes/no response.

- The Consumer System* submits a request for biometrics-based fingerprint verification.
- The Provider System** receives the request.
- The Provider System validates the request and sends a fault message in the case of an invalid request.
- In the case of a valid request, the Provider System performs a fingerprint-based search.
- If a matching record is found, the Provider System sends a positive response to the Consumer System.
- If no matching records are found, the Provider System sends a negative response to the Consumer System.
- The Consumer System receives the positive or negative response.

**The Consumer System is any law enforcement, courts, criminal history, corrections, jail, etc. system which requires fingerprint identification as part of its designed business process flow.*

***The Provider System is any system which can provide biometrically based identification. In most of the cases, the Provider System is a system which has the capability to store a collection of biometric objects and identifiers.*

The following diagram represents the alternative process flow in a graphical format.

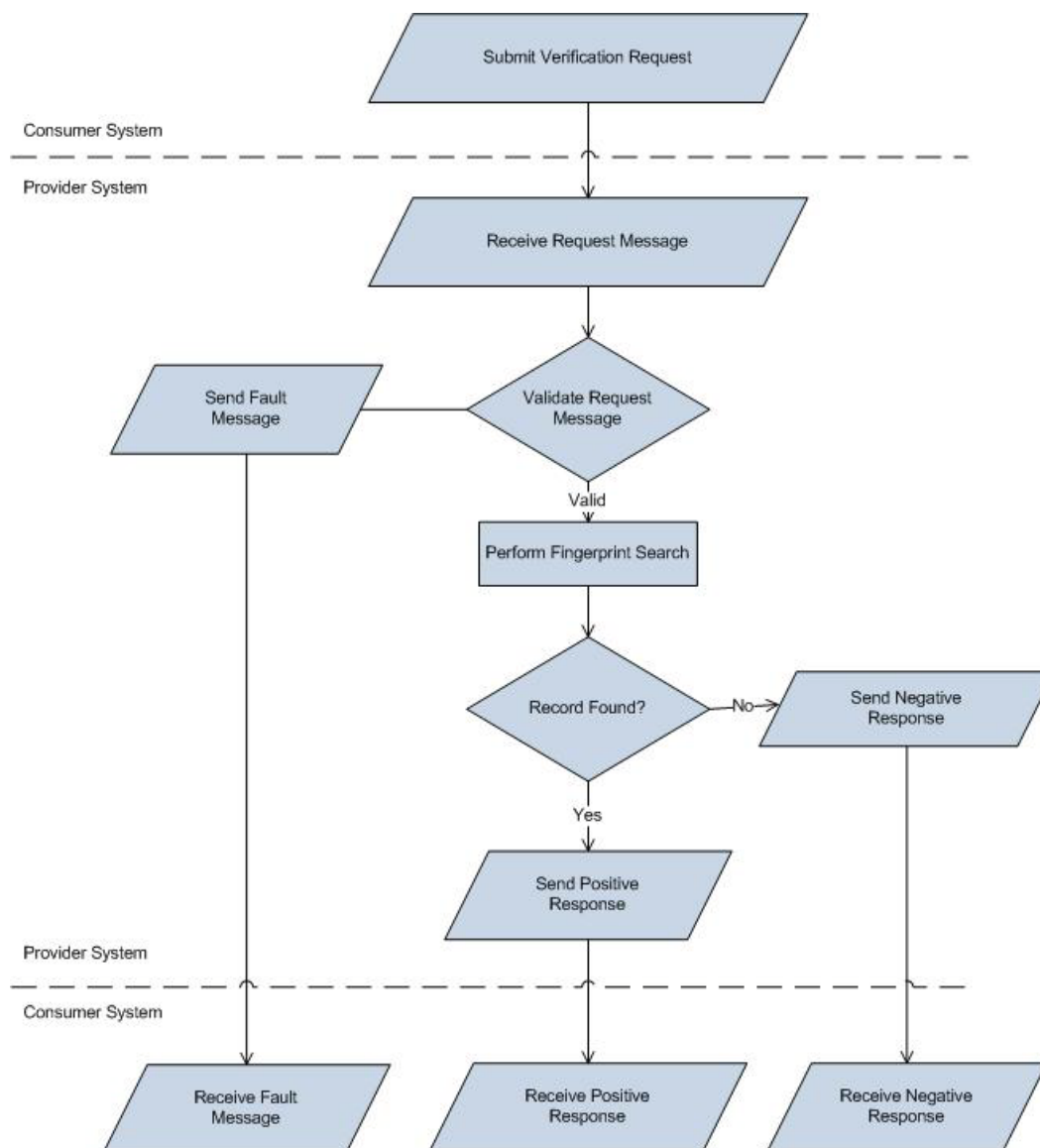


Figure 2: Alternative Process Flow Diagram

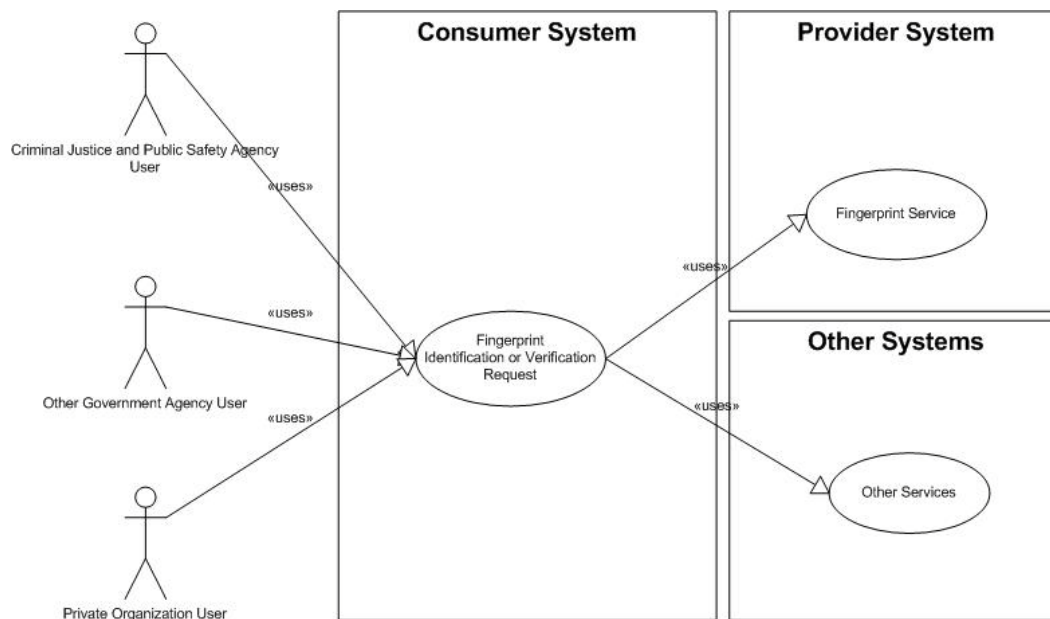
The following fault conditions could exist for the primary and alternative process flows:

1. The service is not operational at the time of the inquiry.
2. The inquiry does not contain all of the required data elements.
3. The inquiry does not contain valid entries for one or more data elements.
4. The fingerprints are not of sufficient quality to perform the biometric search.

The Fingerprint Service could implement a number of profiles which are not mutually exclusive. These profiles are dependent on the information model of the service. The current version of the service leverages the Electronic Biometric Transmission Specification (EBTS) National Information Exchange Model (NIEM) Information Exchange Package Documentation (IEPD) created by the Criminal Justice Information Services Division (CJIS) of the Federal Bureau of Investigation (FBI). Provided below is information regarding the various profiles and how they are implemented in the current version of the service utilizing EBTS.

1. The Fingerprint Service can specify the minimum and maximum number of fingerprints required. Currently, it requires two to ten prints leveraging EBTS Type-4 or Type-14 Records.
2. The Fingerprint Identification Service can specify the particular fingerprints required (e.g., left index, right thumb). Currently, it requires EBTS Type-4 or Type-14 Records.
3. The Fingerprint Identification Service can specify whether the fingerprint impressions must be rolled or flat. As defined in the EBTS, Type-4 Records are for rolled prints and Type-14 Records are for flat prints.
4. The Fingerprint Identification Service can specify the minimum resolution of the fingerprint images (e.g., 500 ppi). Currently, EBTS supports a TransactionImageResolutionDetails tag that can be set to specify the resolution of the images in a transaction.

The following use case and sequence diagrams illustrate the exchanges involved when invoking the Fingerprint Service. The Fingerprint Service will likely be invoked by an intermediary service that lies between the requestor and the service. As a result, the Consumer System will most likely implement a composite service which will invoke the Fingerprint Service. These diagrams also show how subsequent services may be invoked based upon the output of the service.

**Figure 3: Use Case Diagram**

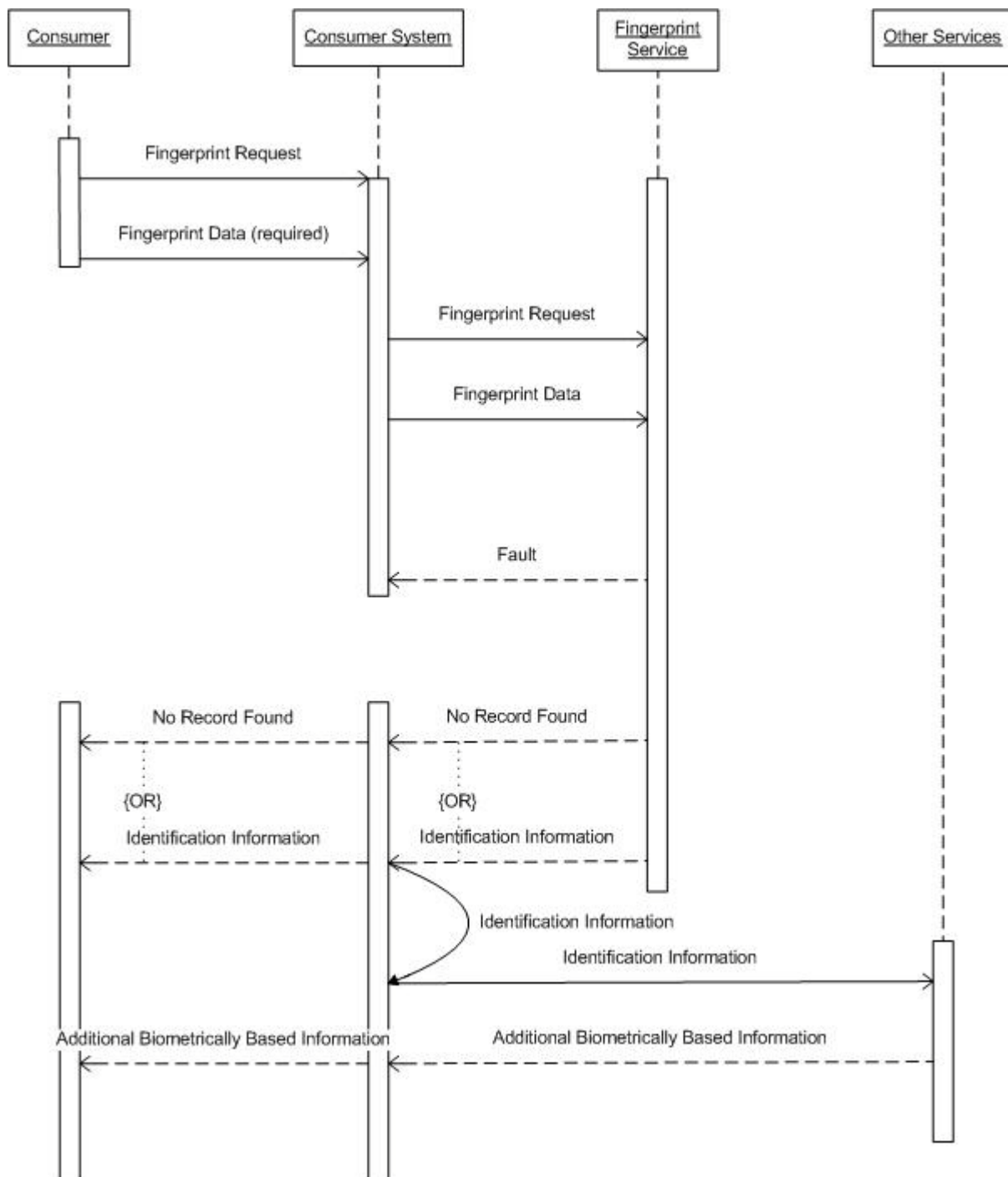


Figure 4: Sequence Diagram

4. Service Interoperability Requirements

4.1 Service Assumptions

- All messages exchanged are stored in a log file for auditing purposes.

- It is expected that the Fingerprint Service would be used as a component of a composite service. The composite service would provide the context for the response (e.g., criminal history information, warrants information, inmate information).
- It is expected that common capabilities such as audit and authentication will be handled by other services and be part of larger, composite services.

4.2 Service Dependencies

No dependencies have been identified at this time.

4.3 Execution Context

The service design will follow the GRA Execution Context Requirements.

4.4 Policies and Contracts

- Consumer and provider organizations will use Memoranda of Understanding (MOUs), Non-Disclosure Agreements (NDAs), or other types of agency agreements, as appropriate.

4.5 Security

- The service must adhere to the rules of the CJIS Security Policies.
- All messages exchanged between consumer and provider organizations should only contain SBU information.
- The MOUs between consumer and provider organizations will regulate security requirements.

4.6 Privacy

- The MOUs between consumer and provider organizations will further define specific privacy requirements.

4.7 Other Requirements

No other requirements have been identified at this time.

5. Additional Information

- This service may be orchestrated with other services using a biometrically based identification number received as part of the service response to obtain criminal history record information, active arrest warrants, sex offender registration information, and other registered offender information. In this scenario, the Fingerprint Service would be used as a component in a composite service; for example, the Fingerprint Service could be part of a composite service which provides criminal history record information. The biometrically based identification provided by the Fingerprint Service will be used by the composite service to obtain criminal history information from multiple repositories, such as local, regional, state, or federal.

6. Information Model

The Fingerprint Service will leverage the Electronic Biometric Transmission Specification (EBTS) National Information Exchange Model (NIEM) Information Exchange Package Documentation (IEPD) created by the Criminal Justice Information Services Division (CJIS) of the Federal Bureau of Investigation (FBI).

The EBTS is the method by which the FBI supports the exchange of biometric data used to facilitate the determination of the personal identity of a subject from fingerprint, palm, facial, or other biometric information across criminal justice agencies or organizations that use an Automated Fingerprint Identification System (AFIS) or related systems nationwide.

These biometric specifications are standards for electronically encoding and transmitting biometric image, identification, and arrest data. The FBI EBTS is comprised of the biometric standards entitled *Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information (ANSI/NIST-ITL 1-2007)*, which are composed by the American National Standards Institute (ANSI) in correspondence with the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). These standards define the content, format, and units of measurement for the exchange of biometric information.

The EBTS defines the following service areas.

- Identification Service Area
- Verification Service Area
- Information Service Area
- Investigation Service Area
- Notification Service Area
- Data Management Service Area
- Other Biometric Services Area

The Fingerprint Service utilizes the EBTS Identification and Verification Service Areas.

There are several types of transactions for each of these service areas that are accepted by the FBI. It is required that the sender designates the Type of Transaction (TOT) in the Type-1 Record to specify which process is to be followed.

Provided below are the types of transactions for the EBTS Identification and Verification Service Areas.

Identification Service

- Ten-Print Fingerprint Identification Submissions
- Latent Fingerprint Identification Submissions
- Rapid Fingerprint Identification Search Submissions*
- International Terrorist Identification Submissions*
- Disposition Fingerprint Identification Submissions*

Verification Service

- Fingerprint Verification Submissions*

**Denotes future capabilities identified in the EBTS.*

The list below represents the ANSI-NIST record types supported by the EBTS:

Type-1 Header Record

Record required for each transaction, providing information describing the type and use or purpose for the transaction involved, a listing of each logical record included, the original source of the physical record, among other information items.

Type-2 Record

Records containing textual fields providing identification and descriptive information associated with the subject of the transaction.

Type-4 Record

Records used to exchange high-resolution, grayscale, fingerprint image data that was scanned at no less than the minimum scanning resolution.

Type-7 Record

Records used to exchange image data that is not elsewhere specified or described in the ANSI-NIST standard, including miscellaneous images such as those pertaining to latent prints, wrists, toes, soles, etc.

Type-9 Record

Records used to exchange geometric and topological minutiae templates and related information encoded from a fingerprint, palm, or latent image. Each record shall represent the processed image data from which the location and orientation descriptors of extracted minutiae characteristics are listed.

Type-10 Record

Records used to exchange facial and image data from scars, marks, and tattoos (SMT) together with textual information pertinent to the digitized image. The source of the image data shall be the image captured from scanning a photograph, a live image captured with a digital camera, or a digitized “freeze-frame” from a video camera.

Type-13 Record

Records used to exchange image data acquired from latent fingerprint or palmprint images. Textual information regarding the scanning resolution, the image size, and other parameters or comments required to process the image are recorded within the record.

Type-14 Record

Records used to exchange variable-resolution fingerprint image data, segmented flat fingerprint data, or major case print data. All fingerprint impressions shall be acquired from a ten-print card, a major case print card, or from a live-scan device. Fingerprint images can be either rolled or plain (including swiped) impressions.

Type-15 Record

Records used to exchange variable-resolution palmprint image data.

Type-16 Record

Records used to exchange test image data.

Type-17 Record

Records used to exchange iris image data.

Type-99 Record

Records used to exchange biometric data that is not supported by other logical record types. This record type supports and is intended to be used for “exotic” biometric data types.

EBTS Inbound Message Requirements

An individual XML inbound transaction contains at least two records: a Header Record (Type-1) and a User Defined Descriptive Text Record (Type-2). Inbound

transactions may also contain several Image Records including Fingerprint Images, User Defined Images, and Facial and SMT Images. Inbound transactions may also contain records pertaining to minutiae information.

The additional record requirements for each record type are as follows:

- Ten-Print Criminal Justice Submissions:
 - 14 Type-4 or Type-14 Records
 - 10 Rolled Impressions
 - 4 Sets of Plain Impressions
 - 0–20 Type-14 Major Case Print Images
 - 0–8 Type-15 Palmprint Records
 - 0–n Type-10 Records Containing Photos
 - 0–2 Type-17 Iris Image Records
 - 0–n Type-99 CBEFF Records
- Ten-Print Non-Criminal Justice Submissions:
 - 14 Type-4 or Type-14 Fingerprint Image Records
 - 10 Rolled Impressions
 - 4 Sets of Plain Impressions
 - OR 3 Type-14 records (non-criminal justice purposes only)
 - 2 Plain Simultaneous Four Finger Impressions
 - 1 Plain Left and Right Thumb Impression
 - OR 2–10 Type-4 or Type-14 Flat or Rolled Images AND
 - 0–12 Type-14 Major Case Print Images AND
 - 0–8 Type-15 Palmprint Records
 - 0–n Type-10 Records Containing Photos
 - 0–2 Type-17 Iris Image Records
 - 0–n Type-99 CBEFF Records
- Ten-Print Searches:
 - 1–14 Type-4 or Type-14 Fingerprint Image Records
 - OR 1–10 Type-9 Fingerprint Features Records
- Latent Submissions:
 - 1–14 Type-4 or Type-13 Fingerprint Image Records
 - 1–10 for Latent Submissions
 - 14 for Comparison Ten-Print Fingerprint Submissions
 - 14 for Major Case Submissions
 - OR 1–n Type-7 Records

- Latent Searches:
 - 1–10 Type-4 Fingerprint Image Records
 - OR 1–10 Type-13 Fingerprint Image Records
 - OR 1–10 Type-7 Records
 - 1–10 Type-9 Features Records
- Electronic Requests to Upgrade Fingerprint Images:
 - 14 Type-4 or Type-14 Fingerprint Image Records

EBTS Response Message Requirements

An individual XML outbound transaction contains at least two records: a Header Record and a User Defined Descriptive Text Record. Information pertaining to the actual response will be contained within the User Defined Descriptive Text Record. The response message may also contain Fingerprint Images, User Defined Images, Facial and SMT Images, and Minutiae Information Records.

The User Defined Descriptive Text Record of a response message will contain a Transaction Response Data Section, which has information specific to an EBTS response transaction, including fields specifying any action or direction for the user to take upon receiving the transaction, error messages, and other detailed information pertaining to the results of a search.

Additional records that may be returned by the responses are as follows:

- Ten-Print Submission Responses:
 - 0–1 Type-10 Photo record containing the most recent mug shot
- Ten-Print Search Responses:
 - 0–14 Type-4 or Type-14 Fingerprint Image Records (SRT only)
 - 0–1 Type-10 Photo record containing the most recent full frontal photo (RPSR only)
- Latent Submission Responses:
 - 0–14 Type-4 or Type-14 Fingerprint Image Records (LSR only)
- Latent Search Responses:
 - 0–n Type-4 or Type-14 Fingerprint Image Records

- Remote Requests for Fingerprint Image Responses:
 - 0–14 Type-4 or Type-14 Fingerprint Image Records (IRR only)
 - 0–14 Type-9 Features Records
 - 0–8 Type-15 Palmprint Images
 - 0–2 Type-17 Iris Images
 - 0–1 Type-7 or Type-13 Latent Images
- Criminal Subject Photo Request Response:
 - 1–10 Type-10 Image Records

7. Service Model

7.1 Data Inputs

- FingerprintRequest

The logical FingerprintRequest data input, used by both synchronous and asynchronous processes, uses the EBTS IEPD and contains Type-1, Type-2, Type-4, or Type-14 Records, and, optionally, Type-7 Records. The child element of the document root will always be `itl:NISTBiometricInformationExchangePackage` to conform to the EBTS and ITL.

The Type-2 Record contains information regarding the request, including instructions for processing the request such as the Record Retention Indicator.

- FingerprintResponse

The logical FingerprintResponse, which is used as a data input in an asynchronous process, uses the EBTS IEPD and contains Type-1, Type-2, Type-4, or Type-14 Records, and, optionally, Type-7 Records. The child element of the document root will always be `itl:NISTBiometricInformationExchangePackage` to conform to the EBTS and ITL.

The User Defined Descriptive Text Record (Type-2) of a response message will contain a Transaction Response Data Section, which has information specific to an EBTS response transaction, including fields specifying any action or direction for the user to take upon receiving the transaction, error messages, and other detailed information pertaining to the results of a search. The response could be any of the following:

- o I – IDENTIFICATION MADE
- o N –NO IDENTIFICATION MADE
- o P – PENDING
- o R – RED

- o Y – YELLOW
- o G – GREEN

- FingerprintFault

The logical FingerprintFault, which is used as a data input in an asynchronous process, uses the EBTS IEPD and contains Type-1 Header Records and Type-2 Records with information about the error. The underlying element under the root will always contain `itl:NISTBiometricInformationExchangePackage` to conform to the EBTS and ITL. For Faults, the TOT code or Transaction Category Code based on the defined enumerations from the EBTS and ANSI-NIST under the Type-1 Header Record will be “ERRT – TRANSACTION ERROR”. The User Defined Descriptive Text Record (Type-2) of a response message will contain error messages and other detailed information pertaining to the results of a search.

7.2 Data Outputs

- FingerprintResponse

The logical FingerprintResponse is used as a data output in a synchronous process.

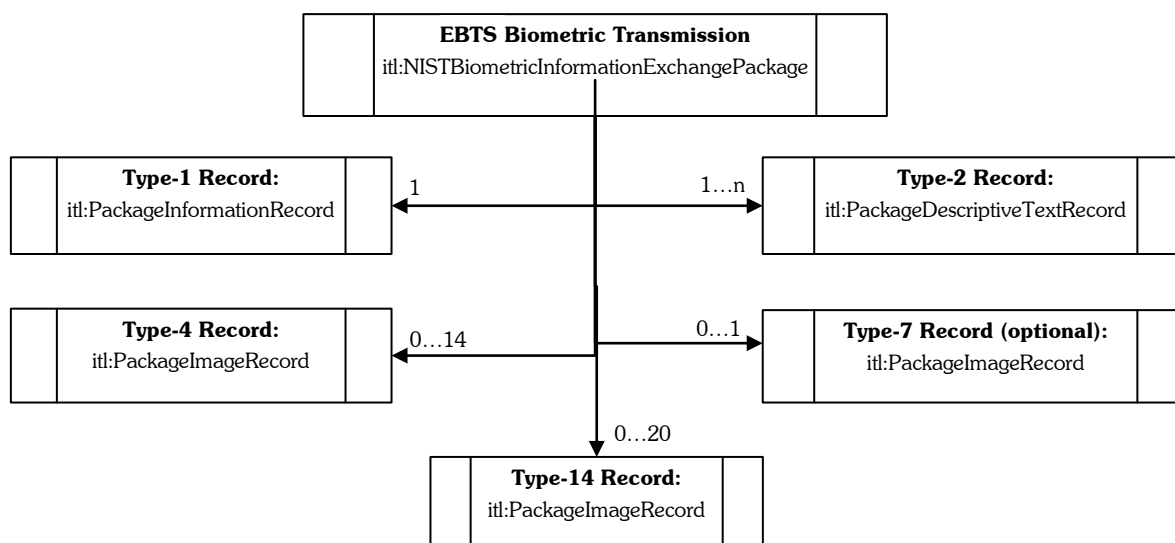
- FingerprintFault

The logical FingerprintFault is used as a data output in a synchronous process.

7.3 EBTS Message Structure

The EBTS message structure used in the FP Service information model is depicted below. The information model adapts the Type-1, Type-2, Type-4, or Type-14 and, optionally, Type-7 Records. For additional information, please refer to the ANSI/NIST-ITL 2-2008 XML version² and the EBTS IEPD documentation.

² <http://fingerprint.nist.gov/standard/xml/index.html>



7.4 Data Provenance

The data exchanged by this service would originate at the provider organization. The provenance of the data will be restricted to the data available from the specific provider organization.

8. Behavior Model

There are two types of patterns implemented by the Fingerprint Service and described in the actions below.

8.1 Synchronous

Under the synchronous process, a response is returned within the same transaction as the request.

8.2 Asynchronous

Under the asynchronous process, a response is returned outside of the request transaction and is sent back to the consumer once it is ready. In order for this process to work, it is assumed that the consumer has a Web service enabled on its end to receive the returned response.

8.3 Action Model

Action Name	RequestSyncFingerprint
Action Purpose	
Allows consumer systems to request fingerprint identification or verification in a synchronous communication pattern.	
Action Inputs	Action Outputs
FingerprintRequest	FingerprintResponse, FingerprintFault
Action Provenance	
The provenance of this action is the same as the provenance of the service.	

Action Name	RequestAsyncFingerprint
Action Purpose	
Allows consumer systems to request fingerprint identification or verification in an asynchronous communication pattern. This action requires WS-Addressing “Correlation ID” and “Reply To” properties to determine the destination for the response.	
Action Inputs	Action Outputs
FingerprintRequest	None
Action Provenance	
The provenance of this action is the same as the provenance of the service.	

Action Name	SubmitAsyncFingerprintResponse
Action Purpose	
This action will be used to communicate information regarding the fingerprint identification response in an asynchronous pattern. The service will receive the Fingerprint Identification Response from the repository application or service. This action uses the WS-Addressing “Correlation ID” and “Reply To” properties from the initial request to determine the destination for the response.	
Action Inputs	Action Outputs
FingerprintResponse	None
Action Provenance	
The provenance of this action is the same as the provenance of the service.	

Action Name	SubmitAsyncFingerprintFault
Action Purpose	
This action will be used to communicate faults and errors regarding the fingerprint identification request in an asynchronous pattern. The service will receive the Fingerprint Identification Fault from the repository application or service. This action uses the WS-Addressing “Correlation ID” and “Reply To” properties from the initial request to determine the destination for the fault.	
Action Inputs	Action Outputs
FingerprintFault	None
Action Provenance	
The provenance of this action is the same as the provenance of the service.	

8.4 Process Model

This section contains diagrams providing additional information on how each of the business scenarios can be implemented by invoking the actions of the service utilizing the synchronous and asynchronous patterns.

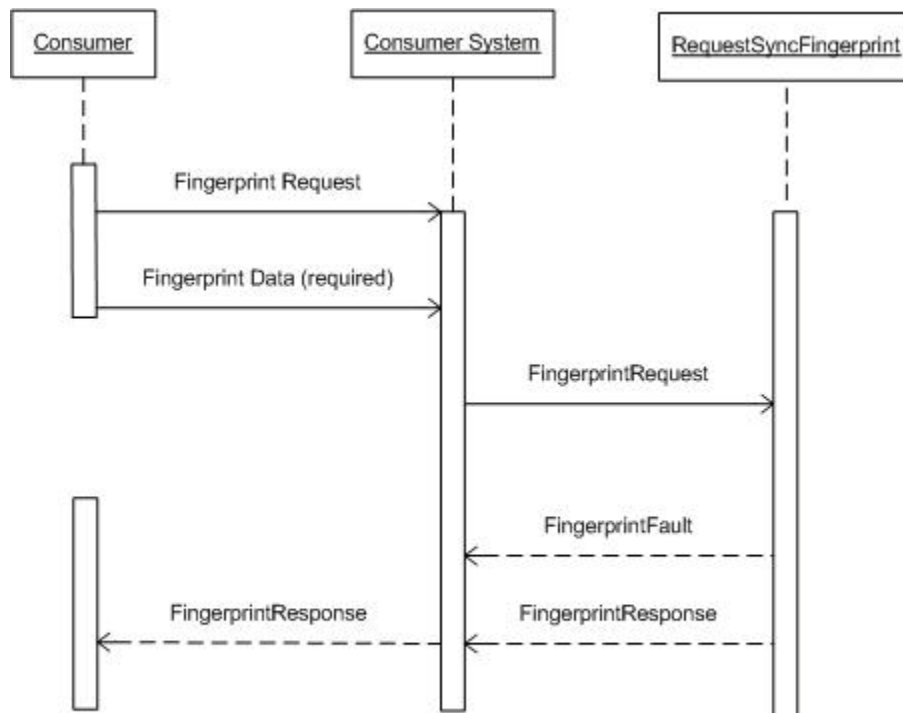


Figure 5: Synchronous Pattern Sequence Diagram

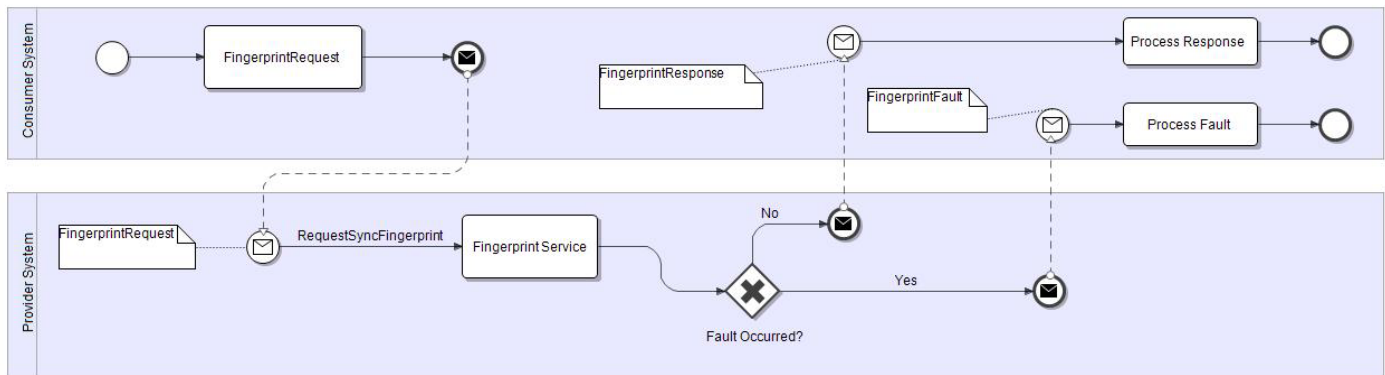


Figure 6: Synchronous Pattern BPMN Diagram

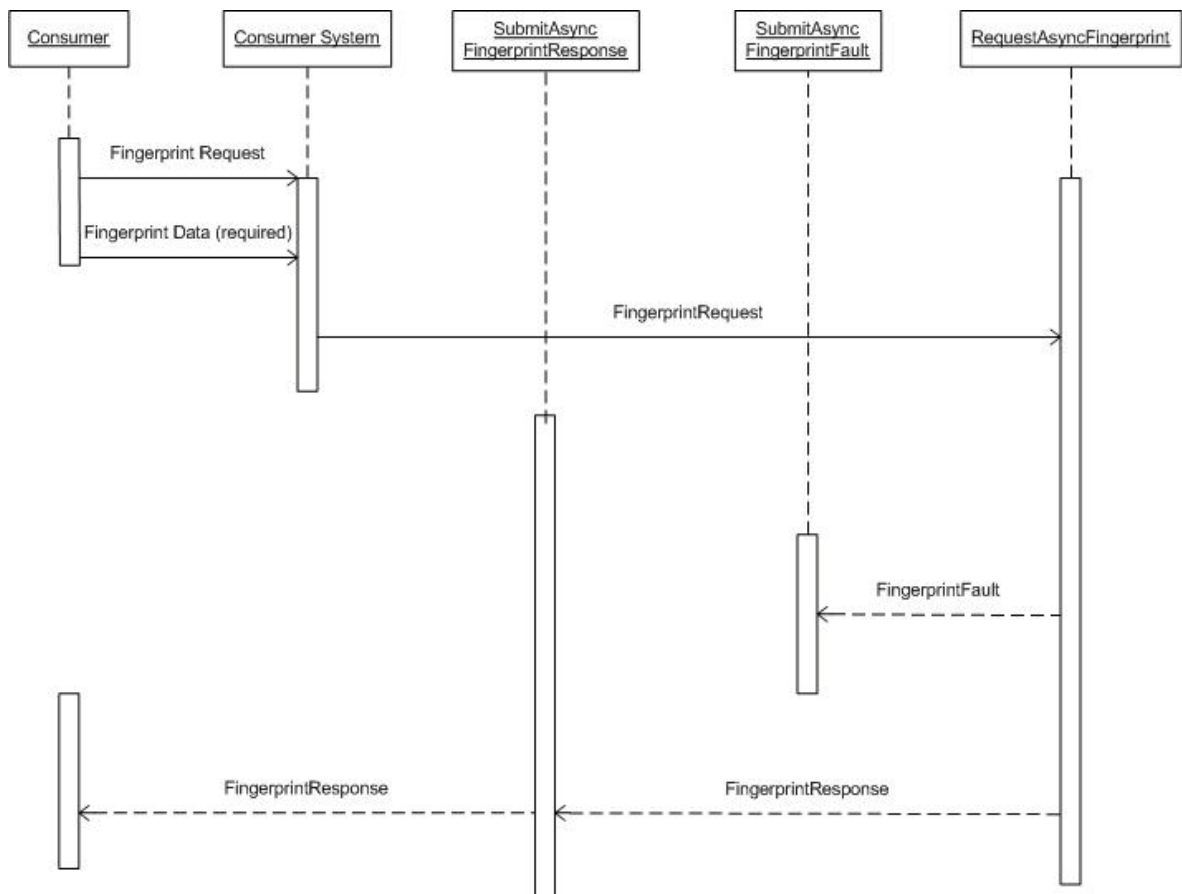


Figure 7: Asynchronous Pattern Sequence Diagram

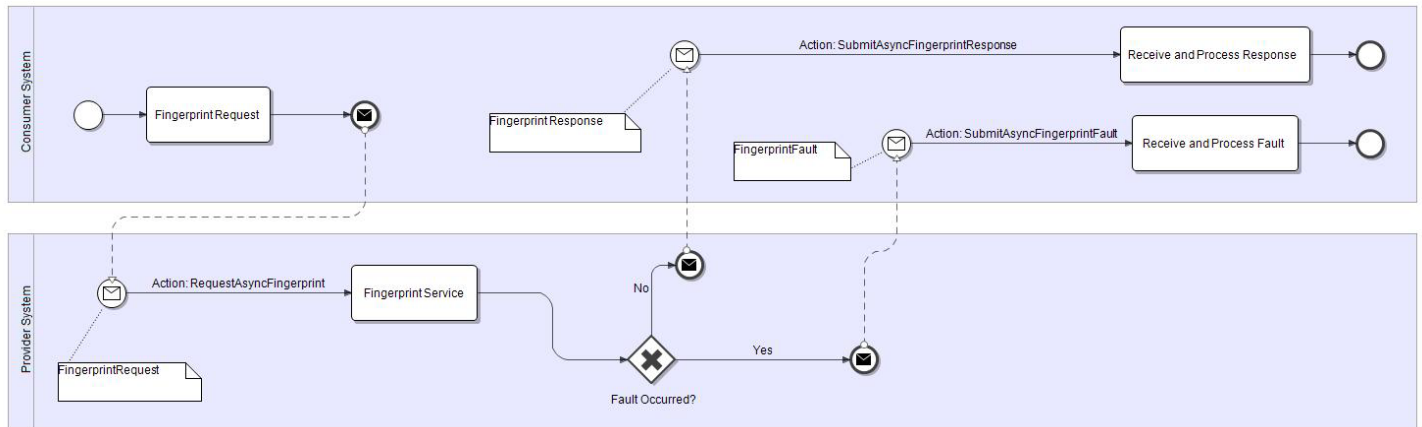


Figure 8: Asynchronous Pattern BPMN Diagram

Appendix A—References

Global Reference Architecture Web Site	http://www.it.ojp.gov/globaljra
CJIS Security Policy	The CJIS Security Policy is considered to be Sensitive But Unclassified (SBU) material. This policy may not be posted to a public Web site, and discretion must be exercised in sharing the contents of the policy with individuals and entities who are not engaged in law enforcement or the administration of criminal justice. A copy may be obtained by contacting the state's CJIS Systems Officer (CSO).
EBTS	A version of the EBTS IEPD leveraged by this service specification is included in this package. For more information, please refer to http://www.fbibiospecs.org/
ANSI/NIST Standard	http://fingerprint.nist.gov/standard/

Appendix B—Glossary

ANSI	American National Standards Institute
CJIS	Criminal Justice Information Services
EBTS	Electronic Biometric Transmission Specification
FBI	Federal Bureau of Investigation
ID	Identifier
IEPD	Information Exchange Package Documentation
NIEM	National Information Exchange Model
NIST	National Institute of Standards and Technology
WS-SIP	Web Services Service Interaction Profile

Appendix C—Document History

Date	Version	Editor	Change
05/04/2009	0.1.01	Iveta Topalova, James Dyche	Initial version
07/01/2009	0.1.02	Iveta Topalova	Revised after meeting with subject-matter experts
07/20/2009	0.1.03	Iveta Topalova	New revision
09/05/2010	0.1.04	Don Dinulos	Updated per new information received regarding EBTS
10/29/2010	0.1.05	Don Dinulos	Created schemas and samples based on new draft version of EBTS
01/22/2010	0.9.1	Don Dinulos, Collin Evans, Iveta Topalova	Updates based on newly released EBTS IEPD; preparation for final release
02/05/2010	0.9.2	IJIS Institute	Technical edit
02/22/2010	0.9.3	Iveta Topalova, Don Dinulos, Collin Evans	Final version
07/11/2011	1.0.0	Collin Evans	Changed JRA references to GRA
04/2012	1.0.0	Global Standards Council (GSC)	Global Advisory Committee approved

About Global

www.it.ojp.gov/global

The Global Justice Information Sharing Initiative (Global) serves as a Federal Advisory Committee to the U.S. Attorney General on critical justice information sharing initiatives. Global promotes standards-based electronic information exchange to provide justice and public safety communities with timely, accurate, complete, and accessible information in a secure and trusted environment. Global is administered by the U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance.

For more information on Global and its products, including those referenced in this document, call (850) 385-0600 or visit <http://www.it.ojp.gov/GIST>.

About GSC

www.it.ojp.gov/gsc

In accordance with the founding principle of Global, the Global Standards Council (GSC) directly supports the broadscale exchange of pertinent justice and public safety information by promoting standards-based electronic information exchanges for the justice community as a whole. Specifically, the GSC develops, maintains, and sustains the standards—including this particular standard—associated with these aforementioned information exchanges. To further foster community participation and reuse, the GSC also receives, evaluates, and recommends to Global for adoption proposed standards submitted by Global consumers and stakeholders. In turn, the GSC employs an enterprise architecture approach for developing and maintaining the cohesive body of Global standards as one Global Standards Package (GSP), which can be accessed at <http://www.it.ojp.gov/gsp>.

<http://www.it.ojp.gov/gsp>
