



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

Global Reference Architecture

Fingerprint Service (FS) Service Interface 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>.

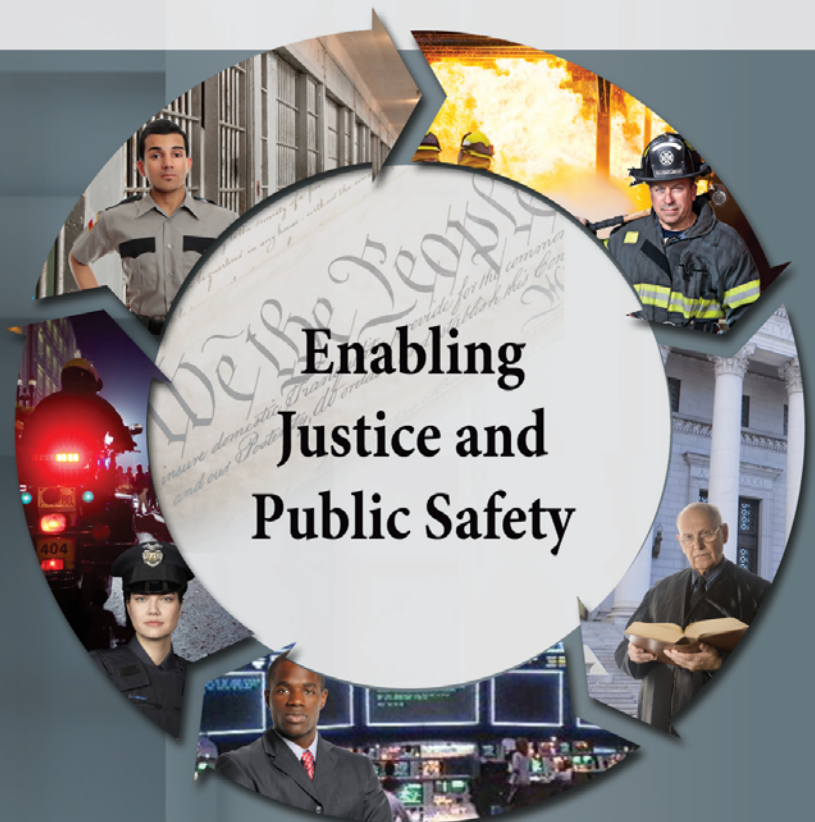


Table of Contents

1. Document Introduction	1
2. Physical Model.....	2
3. Service Interaction Requirements	2
4. Interface Description Requirements	3
5. Message Exchange Patterns	3
6. Message Definition Mechanisms.....	3
7. Policies and Contracts	3
7.1 Policies	3
7.2 Automated Service Contracts	3
7.3 Nonautomated Service Contracts	3
7.4 Umbrella Agreements	4
8. Security.....	4
9. Privacy.....	4
10. Service Testing.....	4
Appendix A—References	5
Appendix B—Glossary	6
Appendix C—Document History	7

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 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 Interface Description of the TSC Encounter Information Service.

2. Physical Model

The Fingerprint Information Service Interface will implement the following service actions:

- RequestSyncFingerprint
- RequestAsyncFingerprint
- SubmitAsyncFingerprintResponse
- SubmitAsyncFingerprintFault

3. Service Interaction Requirements

Requirements	Mandatory (Yes/No)	Specification
Service Consumer Authentication	Yes	As described in CJIS Security Policy
Service Consumer Authorization	Yes	As described in CJIS Security Policy
Identity and Attribute Assertion Transmission	No	
Service Authentication	No	
Message Nonrepudiation	Yes	WS-Security, XML-Encryption, XML-Signature
Message Integrity	Yes	WS-Security, XML-Encryption, XML-Signature
Message Confidentiality	Yes	WS-Security, XML-Encryption, XML-Signature
Message Addressing	Yes	WS-Addressing
Reliability	Yes	WS-ReliableMessaging
Transaction Support	No	
Service Metadata Availability	Yes	See the metadata.xml file in this package.

Requirements	Mandatory (Yes/No)	Specification
Interface Description Requirements	TBD	
Service Responsiveness	Yes	Within one hour of determination or update of Encounter Information

4. Interface Description Requirements

The service will comply with the GRA WS-SIP.

5. Message Exchange Patterns

Action Name	Message Exchange Patterns
RequestSyncFingerprint	REQUEST-RESPONSE
RequestAsyncFingerprint	FIRE-AND-FORGET
SubmitAsyncFingerprintResponse	FIRE-AND-FORGET
SubmitAsyncFingerprintFault	FIRE-AND-FORGET

6. Message Definition Mechanisms

The service will comply with the message definition mechanisms identified in the GRA Web Services SIP.

In addition, the service will follow the message pattern defined in the Electronic Biometric Transmission Specification (EBTS) Information Exchange Package Documentation (IEPD).

For additional information, please reference <http://www.fbibiospecs.org/>.

7. Policies and Contracts

7.1 Policies

No automated policies have been identified at this time.

7.2 Automated Service Contracts

No automated service contracts have been identified at this time.

7.3 Nonautomated Service Contracts

No nonautomated service contracts have been identified at this time.

7.4 Umbrella Agreements

No umbrella agreements have been identified at this time.

8. Security

The service must comply with the CJIS Security Policy.

The service interaction should be secured by a minimum of 128-bit encryption with NIST or CSE certification of the cryptographic module to ensure it meets FIPS Publication 140-2 for “Security Requirements for Cryptographic Modules” at any Security Level.¹

9. Privacy

The service would comply with any memoranda of understanding (MOUs) in place between entities participating in the exchange.

10. Service Testing

Service testing requirements will be identified as part of the implementation by entities participating in the exchange.

¹ For more information, please refer to <http://csrc.nist.gov>.

Appendix A—References

Global Reference Architecture Web Site	http://www.it.ojp.gov/globalgra
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 Systems
EBTS	Electronic Biometric Transmission Specifications
FBI	Federal Bureau of Investigation
FC	Fusion Center
IAC	Information Analysis Center
ID	Identifier
IEPD	Information Exchange Package Documentation
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	Final 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
04/11/2012	1.0.0	David Gillespie	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>
