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

Global Reference Architecture

Terrorist Screening Center Encounter Information (TSCEI) Service Sender 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.

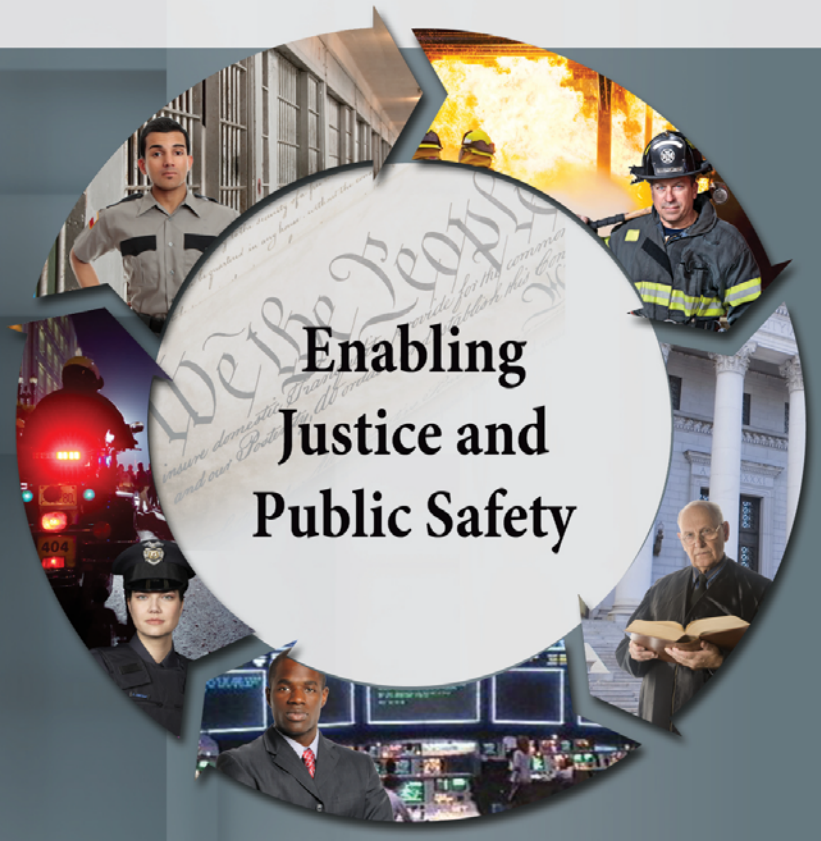

Table of Contents

1. Document Introduction

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 Interface Description of the TSC Encounter Information Service to be implemented by the Terrorist Screening Center.

2. Physical Model

This service will implement the Terrorist Watchlist Person Data Exchange Standard (TWPDES) Message Transaction Specification. In addition, the service will implement the GRA Web Services-Service Interaction Profile (WS-SIP).

This interface is to be implemented by the sender (e.g. Terrorist Screening Center) to receive acknowledgement messages from the receiver (e.g. Fusion Centers). The interface by which the sender submits encounter information to receivers is defined in the TSCEI-Receiver Service Interface Description Document included in this package.

The information flow diagram below depicts the WS SIP-compliant implementation:

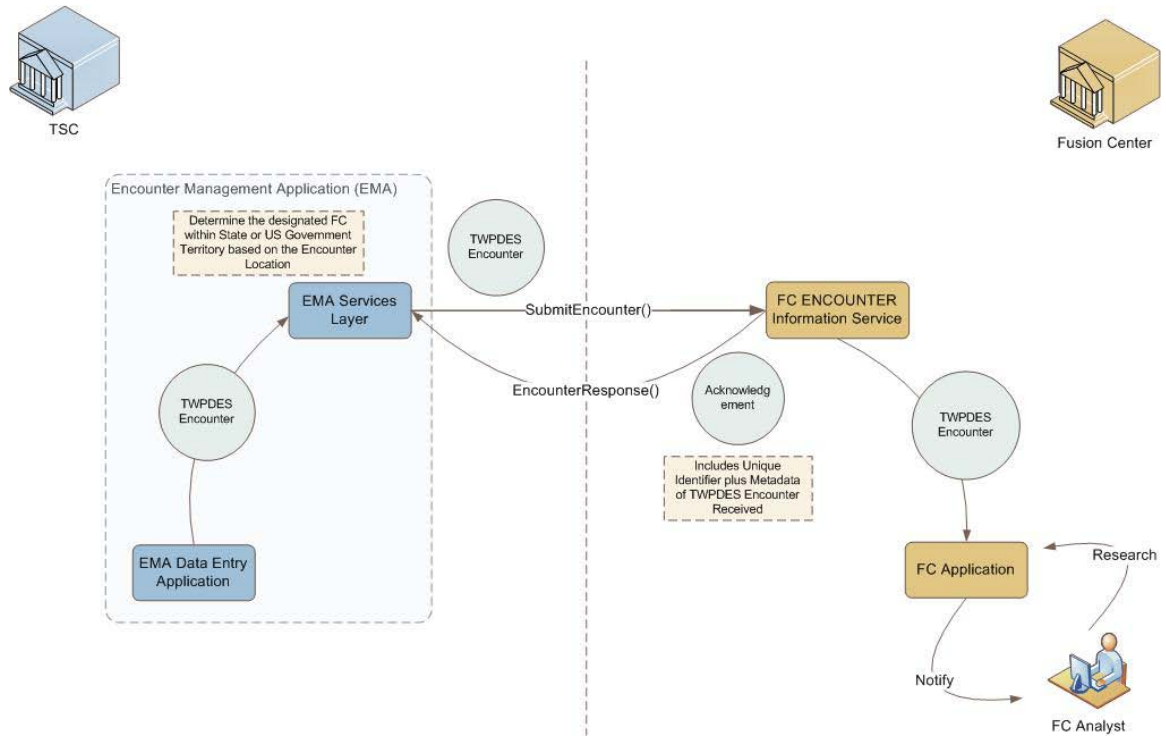

Figure 1: Information Flow Diagram Utilizing WS-SIP

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.
Interface Description Requirements	TBD	
Service Responsiveness	Yes	Within one (1) hour of determination or update of Encounter Information

4. Interface Description Requirements

The service will comply with the GRA WS SIP v1.2.

5. Message Exchange Patterns

The Encounter Information Service uses an asynchronous implementation of the **request-response** message exchange pattern using two one-way, fire-and-forget MEPs. The EMA Services Layer sends an Encounter Message to the Encounter Information Service. The Encounter Information Service sends an Acknowledgement message as a reply.

Action Name	Message Exchange Patters
EncounterResponse	FIRE-AND-FORGET

6. Message Definition Mechanisms

The service will follow the message definition mechanism described in the TWPDES Message Transaction Specification.

For additional information, please reference http://www.niem.gov/TWPDES.php.

7. Policies and Contracts

7.1 Policies

No automated polices 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 will adhere to the security rules required and documented by the Terrorist Screening Center (TSC).

The service will adhere to "Guideline 9: Security" of the *Fusion Center Guidelines* document.

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]

[1] For more information, please refer to http://csrc.nist.gov.

9. Privacy

The service will adhere to "Guideline 9: Privacy and Civil Liberties" of the *Fusion Center Guidelines* document.[2]

The service would also comply with the MOU between TSC and the state and U.S. government territory designated fusion centers.

10. Service Testing

Service Testing requirements will be identified between TSC and the state and U.S. government territory designated fusion centers during service implementation.

[2] For more information, please refer to http://www.it.ojp.gov/documents/fusion_center_guidelines.pdf.

Appendix A—References

Fusion Center Guidelines	http://www.it.ojp.gov/documents/fusion_center_guidelines.pdf
Terrorist Watchlist Person Data Exchange Standard (included in this package)	http://www.niem.gov/TWPDES.php
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).

Appendix B—Glossary

IAC	Information Analysis Center
FC	Fusion Center
TSC	Terrorist Screening Center
EMA	Encounter Management Application
Encounter	An Encounter is an interaction between a person of interest (POI) and law enforcement or screening agencies. A person of interest is one who possesses an identity that is associated with derogatory information residing in one or more systems of record (SOR) containing known and suspected terrorists (KST).
NCIC	National Crime Information Center
JTTF	Joint Terrorism Task Force
TSOU	Terrorist Screening Operations Unit
TSDB	Terrorist Screening Database
KST	Known or Suspected Terrorist File
TWPDES	Terrorist Watchlist Person Data Exchange Standard

Appendix C—Document History

Date	Version	Editor	Change
02/21/2009	0.01.01	Iveta Topalova, Don Dinulos, Charles Carlton	Initial version
03/12/2009	0.01.05	Iveta Topalova	Updates to Service Specification
03/16/2009	0.01.05	Jim Douglas, Sam Ali	Review
03/18/2009	0.01.06	Iveta Topalova	Updates to Service Specification based on review
03/24/2009	0.01.06	Stan Larmee, Mark Korkolis	Review
03/25/2009	0.01.06	Jim Douglas	Review
03/26/2009	0.01.07	Iveta Topalova	Updates to Service Specification based on review
03/27/2009	0.01.08	IJIS Institute	Technical edit and formatting
03/27/2009	0.01.09	Iveta Topalova	Next revision
12/31/2009	0.05.01	Iveta Topalova, Collin Evans	Updates based on information from TSC
01/11/2010	0.9.2	Iveta Topalova	Updates based on review by TSC
01/18/2010	0.9.3	Collin Evans	Minor package revisions
08/30/2010	0.9.4	Collin Evans	Separation of FC service interface and TSC service interface to accommodate asynchronous acknowledgements
07/05/2011	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

This project was supported by Grant No. 2009-DB-BX-K105 awarded by the Bureau of Justice Assistance, Office of Justice Programs, in collaboration with the U.S. Department of Justice's Global Justice Information Sharing Initiative. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the U.S. Department of Justice.