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

Global Reference Architecture

Statewide Automated Victim Information and Notification (SAVIN)

Victim Notification (VN) Service Victim Notification Provider Service Interface (VNPSI) Description Document

Version 1.0.0

December 2012

Global Information Sharing Standard

Global Standards

The collection of Global-recommended normative standards has been developed and assembled into a unified package of composable, interoperable solutions that enable effective information exchange. This collection is known as the Global Standards Package (GSP). GSP solutions are generally focused on resolving technical interoperability challenges but also include associated guidelines and operating documents to assist implementers. The GSP includes 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 are reusable nationwide in order to save time and money and reduce complexity when implementing particular information exchanges with external partners.
- **Global Federated Identity and Privilege Management (GFIPM):** Guidelines and standards for establishing, implementing, and governing security, identity management, and access control solutions to ensure that information can be accessed only securely and appropriately.
- **Global Privacy Technology Framework:** A framework for automating information access controls based on privacy and related policies restricting the use or dissemination of such information.

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.

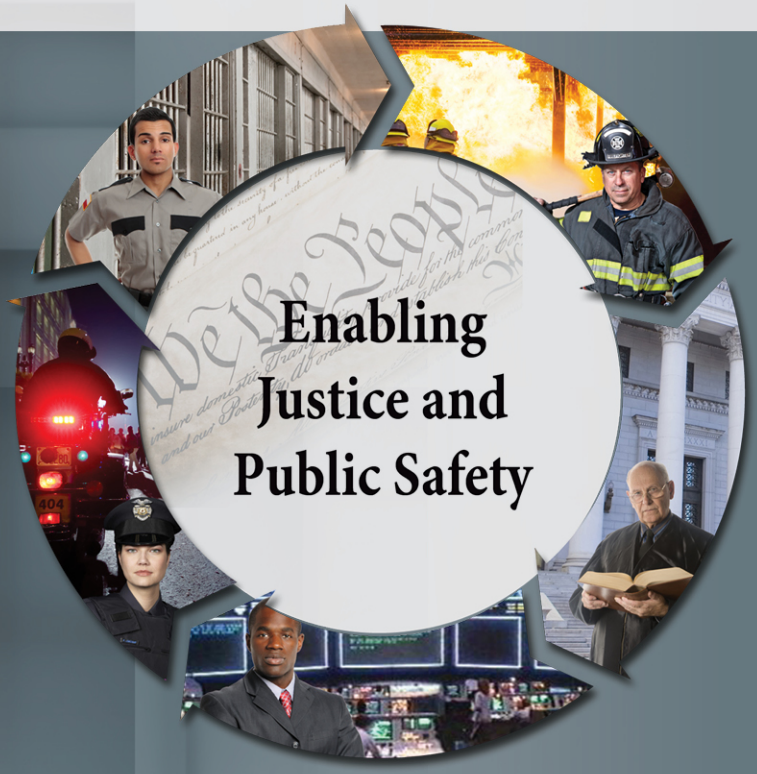

Table of Contents

1. Introduction

This document is designed as a Service Interface Description for the VN Service.

In the context of the Global Reference Architecture (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 to these organizations for sharing information and having 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 that can be described in an open-standard, machine-referenceable format (that is, a format that could automatically be 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 that provide a means of 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 that 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.

The VN Victim Notification Service Provider Service Interface (VNPSI) implements an asynchronous fire-forget pattern to receive an *event notification message* from the Notifying Agency system.

See also the VN Service Description Document provided in the Service Specification Package.

2. Physical Model

This service interface will implement the following actions:

- EventNotification

The service will comply with the GRA Reliable Secure Web Services, Service Interaction Profile version 1.2.

The service will implement the normative requirements stated in the GRA Execution Context Document.

3. Service Interaction Requirements

Requirement	Mandatory	Specification
Service Consumer Authentication	Yes	As described in CJIS Security Policy
Service Consumer Authorization	Yes	As described in CJIS Security Policy
Identity Attribute Assertion Transmission	Yes	GFIPM
Service Authentication	Yes	GFIPM
Message Nonrepudiation	Yes	WS-Security, XML-Encryption, XML-Signature

Requirement	Mandatory	Specification
Message Integrity	Yes	WS-Security, XML-Encryption, XML-Signature
Message Confidentiality	Yes	WS-Security, XML-Encryption, XML-Signature
Message Addressing	Yes	WS-Addressing 1.0
Message Reliability	No	WS-RM
Transaction Report	No	
Service Metadata Availability	No	See the metadata.xml file in this package
Interface Description Requirements	Yes	See Interface Description Requirements section in this document.
Service Responsiveness	Yes	Determined by implementation. As defined by the specific Service-Level Agreement (SLA).

4. Interface Description Requirements

The service will comply with the GRA Reliable Secure Web Services, Service Interaction Profile version 1.2.

5. Message Exchange Patterns

The table below provides information regarding the message exchange patterns under which each of the service actions can be implemented.

Action Name	Message Exchange Pattern
Event Notification	FIRE-AND-FORGET*

**Although this action employs a "fire-and-forget" model, the response message must include WS-Addressing and WS-RM (Web Services Reliable Messaging) metadata. This metadata is used to return an acknowledgement or fault message to the submitter.*

6. Message Definition Mechanisms

The service will comply with the message definition mechanisms identified in the GRA Reliable Secure Web Services, Service Interaction Profile version 1.2.

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.

7.5 Security

- The service implementation must adhere to the rules of the CJIS Security Policies.

- Due to the variety and complexity of the security rules associated with the messages exchanged by the VN Service and the significant differences from one jurisdiction to another, it is recommended that a comprehensive authorization and access control mechanism based on GFIPM be in place for the implementation of this service.

7.6 Privacy

- The memoranda of understanding (MOUs) between participating entities will further define specific privacy requirements.

- Because of the variety and complexity of the privacy rules associated with the messages exchanged by the VN Service and the significant differences from one jurisdiction to another, it is recommended that a comprehensive authorization and access control mechanism based on GFIPM be in place

for the implementation of this service. This would allow implementation of the guidelines defined by the Global Privacy Technical Framework.

- Note that in many cases, simply divulging the existence of information is equivalent to disseminating the information itself. Implementers must take care to ensure that appropriate authorization and access controls are in place even when exchanging seemingly benign flags that indicate information availability.

8. Service Testing

Service Testing requirements will be identified between consumer systems requesting information and provider systems responding to requests.

Appendix A—References

Global Reference Architecture Web Site	http://www.it.ojp.gov/default.aspx?area=nationalInitiatives&page=1015
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

SAVIN	Statewide Automated Victim Information Notification
SBU	Sensitive But Unclassified
WS-Addressing	Web Services Addressing
WS-RM	Web Services Reliable Messaging

Appendix C—Document History

Date	Version	Editor	Change
08/30/2011	0.1.0	Brad Kobishop	Initial version.
02/21/2012	1.0.0	Brad Kobishop	Final review.
06/18/2012	1.0.0	Global Standards Council (GSC) Services Task Team (STT)	Public comment period.
10/18/2012	1.0.0	GSC STT	Service changes received from IJIS—changes incorporated.
12/6/2012	1.0.0	GSC	Approved.
02/01/2013	1.0.0	Global Advisory Committee (GAC)	Approved.

About the Global Advisory Committee

www.it.ojp.gov/global

The Global Advisory Committee (GAC) serves as a Federal Advisory Committee to the U.S. Attorney General. Through recommendations to the Bureau of Justice Assistance (BJA), the GAC supports standards-based electronic information exchanges that provide justice and public safety communities with timely, accurate, complete, and accessible information, appropriately shared in a secure and trusted environment. GAC recommendations support the mission of the U.S. Department of Justice, initiatives sponsored by BJA, and related activities sponsored by BJA's Global Justice Information Sharing Initiative (Global). BJA engages GAC-member organizations and the constituents they serve through collaborative efforts, such as Global working groups, to help address critical justice information sharing issues for the benefit of practitioners in the field.

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 the Global Standards Council

www.it.ojp.gov/gsc

The Global Standards Council (GSC) serves as a Global Advisory Committee (GAC) subcommittee, supporting broadscale electronic sharing of pertinent justice- and public safety-related information by recommending to BJA (through the GAC) associated information sharing standards and guidelines. To foster community participation and reuse, the GSC reviews proposed information sharing standards submitted by Global consumers and stakeholders. Additionally, BJA emphasizes an open, participatory review-and-comment process for proposed standards; please see the Global Justice Tools Web site at www.globaljusticetools.net for more information on this opportunity. BJA-approved standards are developed, maintained, and sustained as one cohesive Global Standards Package (GSP) located at 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, U.S. Department of Justice, in collaboration with the 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.