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

Global Reference Architecture

Execution Context Guidelines

Version 1.3

April 2014

Global Justice Information Sharing Initiative

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.

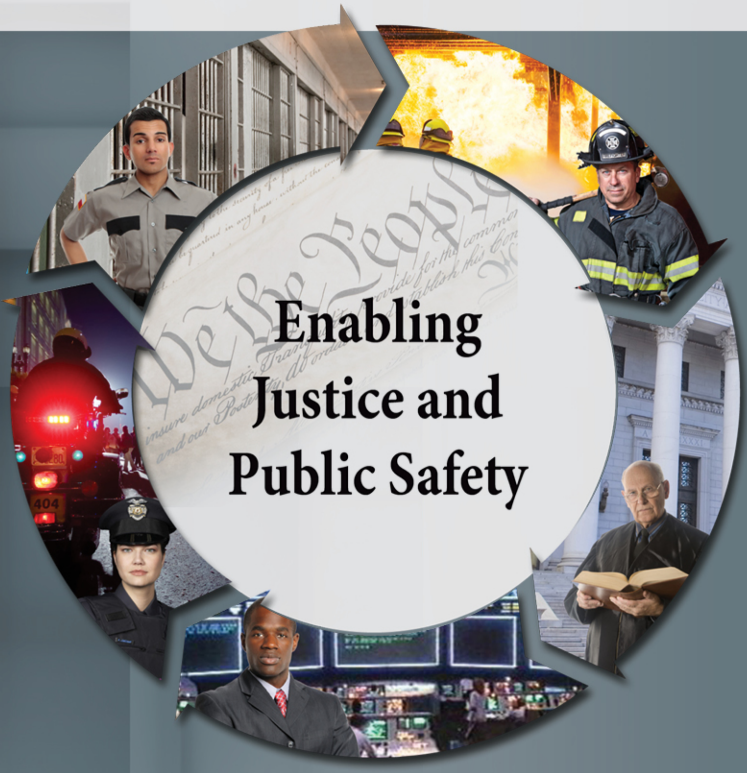


Table of Contents

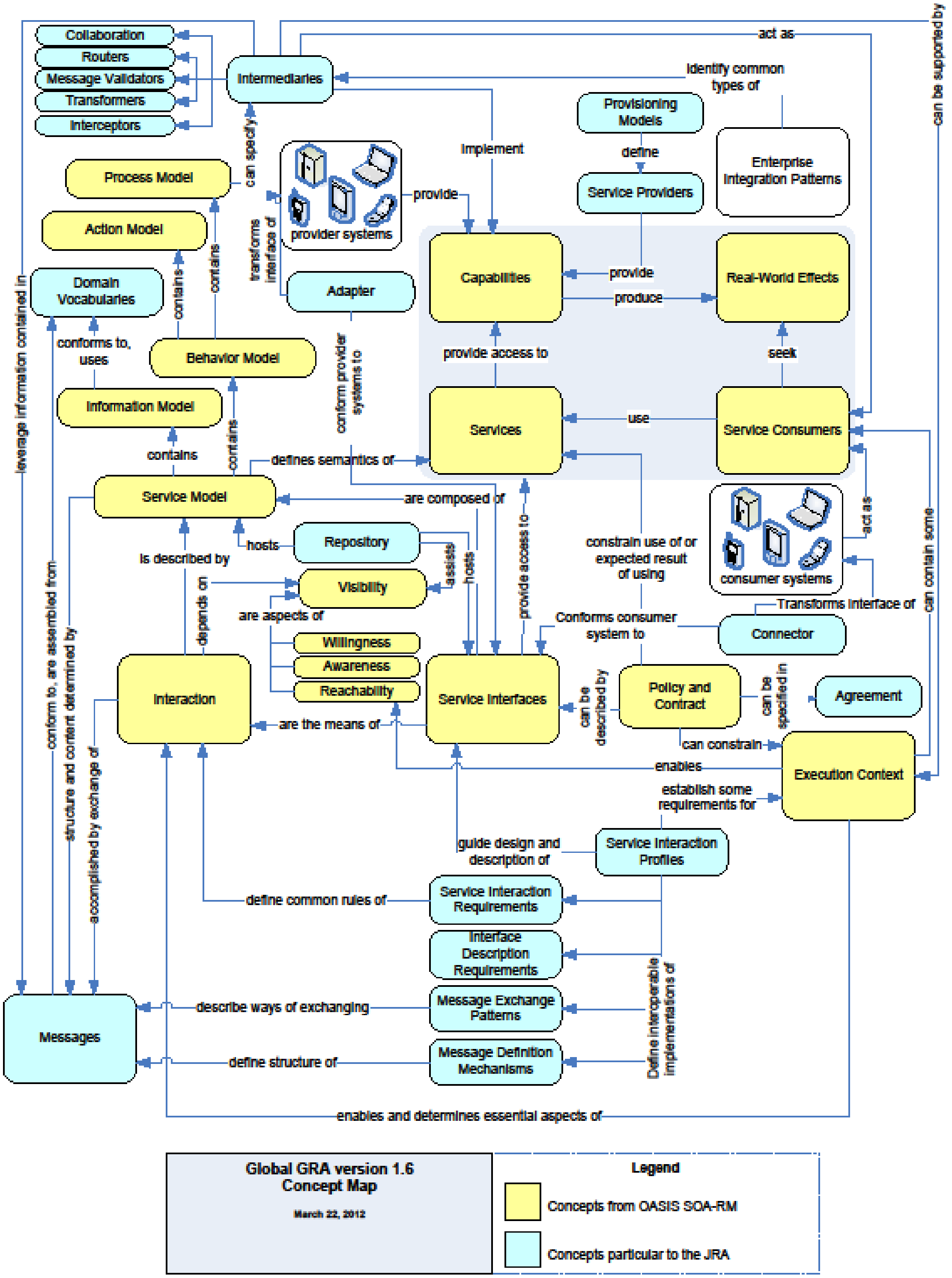
Document Conventions

In this document, use of a bold small-caps typeface, as in this **EXAMPLE**, indicates an important concept or term defined either in the glossary or in the body of the text at the point where the term or concept is first used.

In this document, use of a bold caps typeface, as in this **[EXAMPLE]**, indicates an important resource document which is noted in the Reference Section of this document.

Graphical Overview

The following diagram depicts the concepts, high-level components, and relationships in the Global Reference Architecture Framework Version 1.9.1 [GRA].



1. Introduction

The purpose of this document is to elaborate on the concept of execution context as defined in the Global Reference Architecture **[GRA]**. It will do so by providing guidelines to practitioners overseeing the implementation of a **SERVICE-ORIENTED ARCHITECTURE** (SOA) regarding the implementation of infrastructure to support:

- **REACHABILITY**—The ability of service consumers and services to communicate

- **WILLINGNESS**—The ability of service consumers and service providers to express and enforce their willingness to interact

- **AWARENESS**—The ability of service consumers to be aware of services that may provide a real-world effect that they need

- **INTERMEDIARIES**—The ability to deploy intermediaries, connectors, and adapters

1.1 Usage

The guidelines in this document will be used to plan for the acquisition of hardware and software for organizations adopting the GRA.

1.2 Conformance Targets

The guidelines in this document apply to infrastructure that provides elements of GRA **EXECUTION CONTEXT** for **SERVICES**. For something to conform to the guidelines in this document, it must:

- Fit within the definition of **INFRASTRUCTURE** in the section below.

- Adhere to the constraints specified in each guideline.

2. Concept From the Global Reference Architecture

EXECUTION CONTEXT is the set of infrastructure elements, process entities, policy assertions, and agreements identified as part of a specific, real interaction between a service consumer and a service. Execution context forms a communication and policy path between a service consumer with needs and a service that provides access to a **CAPABILITY** that meets that need.

Execution context is a crucial element for enabling secure interactions between service consumers and services.

For purposes of this document, the term **INFRASTRUCTURE** is defined to be the equipment (tangible objects) and software necessary to form a real, physical, secure communication path (data transmission capability) between a consumer and a service. The communication path may contain equipment and software necessary for the reliable transmission of data (including transient message storage capabilities) and the processing or handling of messages in transit.

2.1 Execution Context

Each service has its own execution context, as defined above. However, in any given GRA implementation, there will be some elements of execution context that are shared across services. The existence of these shared elements provides the implementer with an opportunity to acquire and deploy infrastructure once and share it across multiple services, rather than deploying distinct and separate infrastructure for each service.

Together, the common elements shared across the services infrastructure are the shared execution context and the focus of this paper. This document provides guidance on GRA execution context components for SOA implementers, including identifying components that could be deployed and shared across the multiple execution contexts for numerous service deployments.

3. Implementation Guidelines

The following guidelines are organized into four sections:

- Infrastructure to support **REACHABILITY** (and support for Service Interaction Profiles)
- Infrastructure to support **WILLINGNESS**
- Infrastructure to support **AWARENESS**
- Infrastructure to support **INTERMEDIARIES**, connectors, and adaptors

3.1 Infrastructure to Support Reachability

The GRA defines **REACHABILITY** as "the existence of a communication path or channel that allows a service consumer and service to communicate with one another." This section identifies implementation infrastructure that establishes such a path in terms of communication networks and infrastructure to support reliable messaging transport.

3.1.1 Network Infrastructure

Network infrastructure provides a physical path for service participants to reach out to each other and share the information.

The following types of communication network infrastructures are examples of conformant GRA components that support **REACHABILITY:**

- Local area network (LAN)
- Wide area network (WAN)
- Internet
- Wireless networks

Network Infrastructure Guidelines

Network infrastructure must support the transmission of data among all partners that are providers or consumers of the services and support all the messaging protocols identified in the GRA **SERVICE INTERACTION PROFILES** (SIPs).

Network infrastructure must offer a quality of service (QoS) level sufficient to meet the service-level commitments of all services to which it provides access. QoS includes factors such as reliability, availability, performance, and security.

3.1.2 Infrastructure to Support Message Transport and Reliable Messaging

The messaging infrastructure is fundamental to realizing **REACHABILITY**. Within the context of the GRA, message and transport mechanisms are described and supported by specific Service Interaction Profiles **[ebXMLSIP]** and **[WSSIP]**. A Service Interaction Profile defines a family of industry standards or other technologies or techniques that together demonstrate implementation or satisfaction of the following:

- Service interaction requirements
- Interface description requirements
- Message exchange patterns
- Message definition mechanisms

Message Transport and Reliable Messaging Guidelines

Message transport infrastructure must support the transmission of data among all partners that are providers or consumers of the services and support all the messaging protocols identified in all GRA Service Interaction Profiles in use among the partners.

The following table provides guidelines that apply the Open Systems Interconnection (OSI) Reference Model to the infrastructure to support reachability:

OSI Layers	Layer Description	Infrastructure Guidelines
1	Physical	Network infrastructure must utilize a physical network with a point of presence (POP) for each partner (consumer or provider) with adequate bandwidth.
2	Data Link	
3	Network	Network infrastructure must support network protocols required by SIPs in use among the partners. Network infrastructure should provide for TCP/IP.
4	Transport	
5	Session	Message transport infrastructure must have applications (software) at each partner POP capable of sending and receiving SIP-conformant messages. It must support message persistence and store-and-forward capabilities (reliable messaging) in conformance with the SIPs.
6	Presentation	
7	Application	

3.2 Infrastructure to Support Willingness

According to the GRA, a service must be willing to interact with the consumer—this is called **WILLINGNESS**. The GRA concept of **WILLINGNESS** reflects the scope of interaction permitted between the service consumer and the service provider.

Within an organization's infrastructure, these components of **WILLINGNESS** represent common and shared support across systems, services, and users that provide execution context requirements for critical aspects of any service interaction. For example, the fundamental boundary issues, when interacting *outside* the controlled organizational network and "known" users, include the assurance of:

- Confidentiality
- Integrity
- Availability

There are five target areas for conformance to these guidelines for **WILLINGNESS** of shared infrastructure:

- Network infrastructure security
- Wireless network infrastructure security
- User/system/service identity provisioning and management
- Shared security infrastructure ("authentication")
- Security policy infrastructure ("authorization")

3.2.1 Network Infrastructure Security

The essential backbone of all electronic communication and service interaction is the network infrastructure. Whether one is considering the internal scope of a private network serving a corporate, city, county, or state user community or, as in most instances today, the broader scope of shared networks, there are always threats and security issues that need to be addressed. While limiting one's exposure to external networks and users limits risk, information sharing objectives may be severely hampered when limited to the confines of that controllable network.

In today's increasingly open world, public network infrastructure is widely used and shared by most entities that have access to the Internet. While the Internet provides a convenient network infrastructure, it also introduces many security risks that could potentially interrupt or discourage information sharing. In most external network-sharing scenarios, planning should be done in consideration of public network risks.

Network Infrastructure Security Guidelines

The following elements and mechanisms should be considered as part of the solution (refer to the [SECURITY PRACTICES] document for details on related mechanisms), including:

- Firewalls
- Virtual private networks (VPNs)
- Secure sockets layer (SSL)
- Attack detection and prevention
    - o XML security devices/firewalls
    - o Intrusion detection system (IDS)
    - o Virus detection systems
- Security auditing
- Risk management
- Disaster recovery and business continuity

3.2.2 Wireless Network Infrastructure Security

While wireless technology gives information consumers tremendous mobility, it also introduces various security issues. Wireless networks are susceptible to all of the same vulnerabilities that exist in conventional wired networks. In addition, users may gain access to a network through wireless access points. Depending on the configuration of the network, this may allow malicious users to bypass any protections in place that protect the wired network from external intruders. Further, users (both authorized and unauthorized) may deploy unauthorized equipment that enables access to the wired network that bypasses perimeter protections.

Technologies such as firewalls, VPNs, and virus protection systems are already widely deployed in wired private networks that need to access public networks. These are also needed in a wireless environment, and a judicious implementation of these technologies can help mitigate the risks of deploying a wireless network. **[SECURITY PRACTICES].**

3.2.3 User Identity Provisioning and Management

The following components are identified to support **WILLINGNESS** in an SOA environment.

User Identity Provisioning and Management Guidelines

In order to support **WILLINGNESS**, security infrastructures should be considered that have capabilities for user/system and service identity provisioning and management services, including:

- Directory services—Lightweight Directory Access Protocol (LDAP) and X.500 are open standards that should be considered when implementing directory services.

- Identity management—Identity management implementations should be integrated with directory services to provide shared execution support across multiple applications, systems, and services. Refer to Global Federal Identity and Privilege Management **[GFIPM]** for an example.

- Federated identity management—For services participating in a federated identity context, a protocol and a set of services for establishing a trust relationship between an external identity management provider and one or more relying service providers must be implemented. Refer to **[GFIPM]** for an example.

- Public key infrastructure (PKI)—The most common PKI format standard is X.509. PKI capabilities should be implemented to support authentication, confidentiality, nonrepudiation, and message integrity functions. Note that some GRA SIPs may expressly require this infrastructure for interaction with a service.

3.2.4 Shared Security Infrastructure

Most security and access control policies require an authentication of the identity of the service requestor as the first step in granting/denying access to a service. Commercial products should be considered that implement authentication services for service consumers and service providers. These products include XML security gateways, SOA registry and SOA services management products, open software suites, and SOA platform suites from the major application server vendors.

Shared Security Infrastructure Guidelines

In order to support **WILLINGNESS**, **REACHABILITY,** and **VISIBILITY,** security infrastructures must be considered that have capabilities for providing functions and capabilities, including:

- Authentication—The GRA SIPs require the use of the GFIPM framework, which includes assertions that support a number of open standards specifications for a variety of authentication tokens including X.509 certificates, user name/password, SAML 2.0 Assertions (Federated Identity), and Kerberos.

- Coarse-grained authorization—Most commercial products can implement coarse-grained authorization in addition to authentication capabilities. See Section 3.2.5 Security Policy Infrastructure.

3.2.5 Security Policy Infrastructure (Privacy Policy Enforcement)

Security policy infrastructure represents a collection of software components designed to implement the access control requirements for a service. These authorization functions can be developed with commercial products referred to as entitlement software, fine-grained authorization tools, and/or advanced security and access control (privacy policy) management suites.

A critical success factor for interoperable information sharing for many justice partners is, ultimately, the administrative controls or policy enforcement of who gets access to what data and under what conditions. The concepts of authorization are where privacy enforcement is executed **[PRIVACY POLICY].**

Security Policy Infrastructure Guidelines

In order to support **WILLINGNESS** and **VISIBILITY,** security infrastructures should be considered that have the ability to provide authorization components and functions based on **[GFIPM]** attributes, including the following:

- Fine-grained authorization
- Authorization policy
- Policy Decision Point (PDP)
- Policy Enforcement Point (PEP)
- XML Access Control Markup Language (XACML)
  - OASIS XML-based Policy Assertion Language (PAL)
- Policy authoring tools

3.3 Infrastructure to Support Awareness

Owners, designers, and implementers of service consumer systems need to be aware of services that can produce **REAL-WORLD EFFECTS** within their scope. System implementers also need to understand a service's models (behavior and information) thoroughly to properly implement the consumer system side of service interaction. Finally, owners and designers of service consumer systems need to be aware of the policies and contracts associated with a service if they are to play by the rules. Service registries and repositories provide these capabilities.

Service Registry and Repository Capabilities

A service registry enables a service consumer to locate and access the description as well as other metadata of a service. A repository enables a service consumer to access the service models, policies, and contracts associated with a service.

Repository Capability Guidelines

At a minimum, the infrastructure to support **AWARENESS** must include a query capability that supports the discovery and retrieval of models/artifacts. Repository infrastructure to support awareness also must consider the needs for the following capabilities and functions:

- Life-cycle management interface that manages service models and associated artifacts:
  - Submission of models/artifacts and editing metadata about each artifact
  - Approval of submitted content
  - Deprecation of submitted content
  - Deletion of submitted content

    - Search and location of content
    - Request and acquisition of content (approve the request to consume published content)

- Content management
    - Cataloging (dynamically creating metadata based on artifact content)
    - Validating metadata content upon submission
    - Validating mandatory artifacts upon submission

- Security (authentication, authorization)

- Auditing (submission, queries)

- Event notification
    - Users are notified (e.g., via e-mail) when new content is submitted or existing content is edited.
    - Users are able to choose which notifications to receive; e.g., via filtering mechanisms.

- Federated registry capability—Based on a need for these capabilities, infrastructure should include a repository solution that conforms to the ebXML Registry Services Version 3 **[ebRS3]** specification, which explicitly supports all of the above requirements, and additionally:
    - Federated information management.
    - Multiple ebXML registries may be federated together to appear as a single virtual registry/repository.
        - Seamless information integration and sharing.
        - Allows local autonomy over data.
    - ebXML registry relies on SAML—the federated identity management standard.

3.4 Infrastructure to Support Intermediaries, Connectors, and Adaptors

The GRA identifies a small but significant set of infrastructure components that are core to any GRA implementation. A common services infrastructure should provide support for **INTERMEDIARIES, CONNECTORS,** and **ADAPTORS.**

INTERMEDIARIES are special adapters that mediate information exchanges between consumers and providers, performing such operations as transformations, routing, validation, and message aggregation. Intermediaries reside on an Intermediary Host or broker, which exists in a common space. The intermediary is a component (or set of components linked together) that implements a business process or flow between service consumers and service providers. An intermediary is the mechanism by which the GRA separates the logic of integration from the logic of line-of-business systems, which is a key feature of SOA.

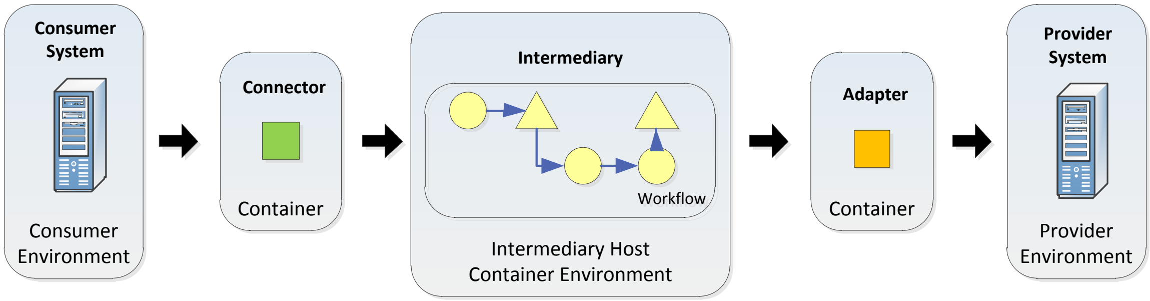
CONNECTORS are components that implement the "consumer" side of a service interaction, typically by observing data changes or "triggers" in a consumer system and initiating a message transmission to an Intermediary. The consumer system essentially "consumes" the service. The connector formulates a message from the service consumer in accordance with the service interface and sends the message to an intermediary service.

ADAPTORS are components that implement the "provider" side of a service interaction, typically by receiving messages from the Intermediary and interacting with the provider system. The provider system essentially "provides" the service. The Adapter receives the message from the intermediary service and adapts the message to the service provider environment.

The concepts of Intermediaries, Connectors, and Adapters are used to ensure the loose coupling and separation of concerns for services. The separation of integration (information flow) logic from the specifics of interacting with each partner system also tends to produce reusable services.

GRA-conformant execution context provides a container environment for intermediaries, connectors (consumers or initiators of interaction), and adapters (providers or recipients of interaction). The communication among these components must adhere to the GRA Service Interaction Profiles (SIPs).

The following figure shows how these components interact with one another in the context of a typical information exchange.



A primary goal of this approach is to avoid point-to-point information exchanges, which tend to be brittle, inflexible, and costly to maintain over time.

The connector formulates information from the consumer system into a message, in accordance with the service interface. The connector sends the message to the intermediary for business processing of the message (e.g., transformations, routing, validation, and message aggregation). A message emerges from the intermediary destined for a provider system, which uses an adapter to manage the interaction between the intermediary and the provider system.

Specific requirement targets for particular shared infrastructure of **INTERMEDIARY** service types are listed in the following sections.

3.4.1 Message Router Support

Message routers are capabilities that receive a message, examine it, and transmit it to one or more destinations based on the message contents or external rules. In general, message routers can be designed to operate on any of the information contained within the message—they may use information about the origin of the message, routing directive information contained within the message, or about the main content of the message itself.

Message Router Support Guidelines

To conform to these guidelines, a messaging infrastructure should support the definition and configuration of components that route messages to their destinations based on rules applied to the contents of messages. By "contents," this requirement means either metadata attached to the message (as envisioned by the message addressing service interaction requirement as defined in the GRA) or the "main" message contents as defined in the service's information model.[1]

3.4.2 Orchestration Support

Defined in the GRA, an **ORCHESTRATION** is a capability that coordinates interaction with multiple services. It is a declarative technique used to compose hierarchical and self-contained, service-oriented business processes that are executed and coordinated by a single conductor. An **ORCHESTRATION** is often implemented using an open industry standard implementation mechanism such as Business Process Execution Language (BPEL), which allows the implementation to be shared across tools and platforms.

Orchestration Support Guidelines

To conform to these guidelines, a messaging infrastructure should support deployment, management, maintenance, and execution of orchestrated business processes defined in **[BPEL].**

[1] These two scenarios are commonly labeled "metadata-based routing" and "content-based routing" in vendors' integration product literature.

3.4.3 Transformer Support

As described in the GRA, **TRANSFORMERS** are services that receive a message and transform it into another format before transmitting it to another destination.

Transformer Support Guidelines

To conform to these guidelines, a messaging infrastructure should support deployment, management, maintenance, and execution of components that transform messages from one format/structure to another. Although there are many proprietary tools for managing transformations, the common infrastructure for any execution context should support transformers defined in terms of **[XSLT]** stylesheets.

3.4.4 Other Intermediaries

The examples of other GRA intermediaries offered below may be employed, as necessary, in accordance with these guidelines.

MESSAGE VALIDATORS are intermediaries that examine a **MESSAGE** to ensure that the contents adhere to established business rules as well as provide quality of service and conformance validation of the message requirements and specifications (e.g., XML standards, or NIEM IEPD Naming and Design Rules).

INTERCEPTORS are intermediaries that receive a message and use the message content to trigger a secondary action; generally, the interceptors pass the message unaltered to the next step in a process. Most interceptors capture information from the message for reporting or analytical purposes.[2]

SECURITY TOKEN SERVICES are services that support trust relationships by defining a set of interfaces that a secure token service may provide for the issuance, exchange, and validation of security tokens. These services are designed to support the creation of multiple security token formats to accommodate a variety of authentication and authorization mechanisms. An issuing security token service takes an input request and, typically, proof of identity and responds with a token that the named identity has requested.

3.4.5 Adaptor and Connector Architectural Options

Note that adaptors and connectors are conceptually distinct components from the systems that they adapt/connect. Nevertheless, it is possible for provider system software to include one or more adaptors as an embedded feature, and similarly for consumer system software

[2] The concept of interceptor defined here is similar to, but separate and distinct from, the notion of an interceptor as defined in the SOAP protocol W3C—SOAP v1.2. **[SOAP]** The definition of this concept in the GRA is not intended to imply any implementation technique or technology.

to include embedded connectors.[3] While this is possible, it is not required, and the appropriateness of embedding these components in the "back-end" systems is largely a factor of the system's technology architecture and, for commercial-off-the-shelf (COTS) software, the vendor's business model. With some COTS software, it may be beneficial (or, in some cases, even necessary) to avoid adding GRA SIP protocols and even XML processing capabilities to application architectures that may not easily support these technologies.

As an alternative to an embedded adapter or connector, it is possible to implement an adapter or connector as a physically separate software component that is not embedded in the provider or consumer system. For this approach to work, consumer and provider systems must be "open"; that is, they must support some mechanism for data access and retrieval that is based on widely available open standards (such as database queries, application programming interfaces, or even file input/output). In addition, the mechanism offered must be well-documented and easily accessible to adaptor/connector developers.

Where practicable, such mechanisms should use NIEM-conformant Information Exchange Package Documentation (IEPD) as the format for data access and retrieval; however, where NIEM conformance is not practicable, clear documentation of the format and supported access/retrieval mechanisms will allow for development and provisioning of nonembedded adaptors and connectors.

4. Operational Considerations

The concept of nonfunctional infrastructure is not addressed explicitly in the GRA, whereas these are capabilities that are not directly related to exposing a real-world effect (i.e., a business-driven service or capability). These considerations are therefore nonfunctional in the sense that they are nonbusiness-specific, but instead are tantamount to the overall quality of business services (QoS) delivery. They are, however, important to the services delivery infrastructure as a whole and, moreover, represent essential candidates for Common Services Infrastructure, where they monitor and/or support the components, capabilities, and requirements for all services and systems within an entity's services delivery framework.

Many of these capabilities ensure aspects of QoS that are addressed within the contracts and agreements of the GRA services paradigm, including availability, scalability, security, maintainability, performance, and supportability. Nonfunctional considerations can be divided into two main categories: (1) execution qualities such as performance, availability, and security, which are observable at run time; and (2) evolution qualities, such as scalability, maintainability, and supportability embodied in the static structure of the software system.

[3] Informally, this approach is sometimes labeled as having the adaptor or connector "baked into" the provider or consumer system, respectively.

4.1 Execution Qualities

4.1.1 Performance and Availability of Common Services Infrastructure

PERFORMANCE represents the amount of useful work accomplished by a computer system compared to the time and resources used relative to time. Depending on the context, acceptable performance may involve one or more of the following metrics:

- Short response time for a given piece of work
- High throughput (rate of processing work)
- Low utilization of infrastructure resource(s)

The performance of any information system should be evaluated in measurable, technical terms, using one or more of the metrics listed above. This way, the performance can be:

- Compared with that of other systems or the same system before/after changes.

- Defined in absolute terms (e.g., for fulfilling the obligation of a service contract or agreement).

AVAILABILITY describes the degree to which a system, subsystem, or infrastructure component is operable and in a ready state at the start of an execution, when the execution is called for at an unknown (i.e., random) time. In other words, availability is the proportion of time a system is in a functioning condition.

To support these operational considerations, operational infrastructures should be implemented that have the following capabilities for runtime systems:

- Monitoring
- Configuration management
- Administrative management

4.1.2 Securing Common Services Infrastructure

Many concepts of operational consideration occur across many or all aspects of the services delivery framework. Security is the foremost of these, inasmuch as it may have operational considerations defined at both the functional and nonfunctional levels of the service infrastructure and many components operating at multiple layers of the service infrastructure stack (e.g., network, session, transport). The security requirements for a functional infrastructure are noted in context elsewhere in this guidelines document.

With respect to nonfunctional requirements for security, they include those aspects of management, agency policies, and individual contracts and agreements that govern the access to and management of the agency's physical infrastructure and personnel, as a whole, as described in **[FIPS 200]**.

To support operational considerations for security, agency, or enterprise, security guidelines should be implemented and documented by each information sharing partner, in accordance with **[FIPS 200]**. The Global Justice Information Sharing Enterprise Statement of Participation (as well as the GFIPM Policies and Procedures and Governance Documents) seek to include these security guidelines and measurements.[4]

4.2 Evolution Qualities

4.2.1 Scalability

The concept of scalability refers to a property or an inherent design of any system, network, or process that indicates its ability to either (1) handle growing amounts of work in a graceful manner or (2) be readily enlarged. QoS infrastructure management capabilities and procedures can be locally implemented with methods that facilitate scalability to include various dimensions, such as:

- Load scalability—The ability of a distributed system to easily expand and contract its resource pool to accommodate heavier or lighter loads. Alternatively, the ease with which a system or component can be modified, added, or removed to accommodate changing load.

- Geographic scalability—The ability to maintain performance, usefulness, or usability regardless of expansion from concentration in a local area to a more distributed geographic pattern.

- Administrative scalability—The ability of an increasing number of organizations to easily share a single distributed system.

Methods of adding more resources for a particular system, process, or application fall into two broad categories:

- Scale vertically—To scale vertically (or scale up) means to add resources to a single node in a system, typically involving the addition of CPUs or memory to a single computer.

- Scale horizontally—To scale horizontally (or scale out) means to add more nodes to a system, such as adding a new computer to a distributed software application.

[4] These documents are future deliverables.

4.2.2 Maintainability and Supportability

These qualities refer to the abilities of technical support personnel to monitor infrastructure components, identify exceptions or faults, debug or perform root cause analysis, and provide hardware or software maintenance in pursuit of solving a problem and restoring the component(s) to service. Incorporating serviceability facilitating features typically results in more efficient product maintenance and reduced costs for technical support.

To support these operational considerations, QoS infrastructure management capabilities and policies should be implemented with features that facilitate serviceability to include:

- Help desk notification of exceptional events
- Network monitoring
- Documentation
- Event logging
- Software upgrade
- Hardware replacement or upgrade planning

5. Incremental Deployment of Common Services Infrastructure

GRA implementers acquire and deploy infrastructure as required by actual operational services and consumers. They should avoid a common misconception that they must make an up-front investment in the complete infrastructure necessary to support all GRA requirements or guidelines. It is generally a better approach to make these investments incrementally, gaining experience and operational support capabilities gradually.

Some implications of this strategy are as follows:

- Common services infrastructure should start with support for simple point-to-point Web services. This support is generally available either through operating system functionality or through simple, inexpensive, often open-source licensed tools.

- The common services infrastructure need not support reliable messaging (RM) source and RM destination components until the first service policy/contract requires reliable messaging (as defined in the service interaction requirements above).

- The common services infrastructure need not support digital certificate issuance, revocation, and provisioning until the first service policy/contract requires message-level authentication, authorization, confidentiality, integrity, or nonrepudiation. To the extent that security requirements can be met at the transport level (i.e., by relying solely on network security), the common services infrastructure does not require digital certificate infrastructure.

- The common services infrastructure need not support intermediaries until the first instance of significant integration logic implementation outside line-of-business applications.

- Common services infrastructure solutions (hardware/software) will best support the strategy if they permit relatively modest initial investments that can scale over time to meet new requirements. The ideal infrastructure platform has all the capabilities identified in these requirements but supports incremental investment in and deployment of components to address those requirements.

- Practitioners should recognize that as common services infrastructure grows in capability and complexity, they will need to provide greater operational support and service management capabilities. These will often involve further infrastructure investments, increased staffing, more formal governance and decision-making, and other support mechanisms.

- The common services infrastructure initially need not support service registry until the first service policy/contract requires service description, service discovery, and service governance via registry infrastructure, which will require further investment.

- Services need not be created from scratch; instead, some services can be created from an organization's existing applications. This refers to the SOA bottom-up approach.

- If organizations have existing services using nonconforming transport protocols, they may be converted into conformant and interoperable services by adding adapters to the services. For example, a JMS service could be converted into a SOAP/HTTP message by utilizing a JMS-to-SOAP/HTTP adapter. The same technique can be applied to a consumer application for other protocol translations. While incremental deployment is a prudent and realistic approach to developing a common services infrastructure, it also introduces concern for life-cycle management of the evolving infrastructure to ensure that the incremental portions integrate with both existing and planned components. This requires a full understanding and a strategic acquisition plan for the larger framework, in addition to a change control plan over the life cycle of the infrastructure.

6. Glossary

Availability

The degree to which a system, subsystem, or infrastructure component is operable and in a ready state at the start of an execution.

Adaptors

Components that implement the "provider" side of a service interaction, typically by receiving messages from the Intermediary and interacting with the provider system.

Awareness

A state whereby one party has knowledge of the existence of the other party. Awareness does not imply willingness or reachability.

Capabilities

Real-world effect(s) that service provider(s) are able to provide to a service consumer.

Connectors

Components that implement the "consumer" side of a service interaction, typically by observing data changes or "triggers" in a consumer system and initiating a message transmission to an Intermediary.

Container

The environment where a service consumer would host its connector(s), a service provider would host its adapter(s,) and the intermediary hosts the intermediaries.

Execution Context

The set of technical and business elements that form a path between those with needs and those with capabilities and that permit service providers and consumers to interact.

Infrastructure

The equipment (tangible objects) and software necessary to form a real, physical, and secure communication path (data transmission capability) between a consumer and a service.

Interceptors

Interceptors are capabilities that receive a message and use the message content to trigger a secondary action; generally, the interceptors pass the message unaltered to the next step in a process.

Intermediaries

Routers and transformers are collectively called intermediaries. This term indicates that routers and transformers generally sit between other services and "mediate" the interaction by managing the transmission of messages between them or by reformatting messages in transit.

Global Reference Architecture (GRA)

The GRA is an abstract framework for understanding significant components and relationships among them within a service-oriented environment. It lays out common concepts and definitions as the foundation for the development of consistent service-oriented architecture (SOA) implementations within the justice and public safety communities. The term refers to the modular architecture that cleanly and appropriately identifies and separates technical and governance layers so that standards can be developed to improve interoperability. The GRA was developed and is maintained by Global; it leverages the work of others, such as the state of Washington, and builds on the work of OASIS.

Messages

The entire package of information sent between service consumer and service (or vice versa), even if there is a logical partitioning of the message into segments or sections.

Message Validators

An intermediary that examines a message to ensure that the contents adhere to established business rules.

Orchestration

A capability that coordinates interaction with multiple services.

Performance

The amount of useful work accomplished by a computer system compared to the time and resources used relative to time.

Reachability

The ability of a service consumer and service provider to interact. Reachability is an aspect of visibility.

Real-World Effects

The actual result(s) of using a service, rather than merely the capability offered by a service provider.

Security Token Services

Services that support trust relationships by defining a set of interfaces that a secure token service may provide for the issuance, exchange, and validation of security tokens.

Services

The means by which the needs of a consumer are brought together with the capabilities of a provider.

Service Interaction Profiles (SIPs)

Defines a family of industry standards or other technologies or techniques that together demonstrate implementation or satisfaction of:

- Service interaction requirements
- Interface description requirements
- Message exchange patterns
- Message definition mechanisms

Service interaction profiles are included in the GRA to promote interoperability without forcing the organization to agree on a single way of enabling service interaction. Each service interface will support a single profile; a service will have multiple interfaces if it supports multiple profiles.

Service-Oriented Architecture (SOA)

Service-oriented architecture is a paradigm for organizing and utilizing distributed capabilities that may be under the control of different ownership domains. It provides a uniform means to offer, discover, interact with, and use capabilities to produce desired effects consistent with measurable preconditions and expectations.

Transformers

A capability that receives a message and transforms it into another format before transmitting it to another destination.

Visibility

The capacity for those with needs and those with capabilities to interact with each other.

Willingness

A predisposition of service providers and consumers to interact.

7. References

BPEL OASIS Business Process Execution Language Specification. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsbpel.

ebXMLSIP GISWG. The GRA ebXML Messaging Service Interaction Profile Version 1.1, April 2011. http://it.ojp.gov/globalgra.

ebRS3 OASIS ebXML Registry Services Specification v3.0. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=regrep, and http://ebxmlrr.sourceforge.net/wiki/index.php/Overview.

FIPS 200 NIST March 2006, Minimum Security Requirements for Federal Information and Information Systems. http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.

GFIPM GSC, GFIPM Metadata Specification, Version 2.0, February 6, 2012. http://it.ojp.gov/gfipm.

GRA Global Reference Architecture Framework, Version 1.9.1, November 2012. http://it.ojp.gov/globalgra.

Privacy Policy GSWG, Implementing Privacy Policy in Justice Information Sharing: A Technical Framework. http://it.ojp.gov/default.aspx?area=globalJustice&page=1239.

SOAP W3C SOAP Version 1.2 Specification. http://www.w3.org/TR/soap/.

WSSIP GISWG. The GRA Web Services Service Interaction Profile Version 1.3, April 2011. http://it.ojp.gov/globalgra.

XSLT WC3 Extensible Style Language Transformations (XSLT) 2.0. http://www.w3.org/TR/xslt20/.

8. Document History

Date	Version	Editor	Change
December 2, 2008	1.0		Initial draft.
April 2011	1.1		Changed JRA to GRA.
November 2012	1.2	Global Standards Council (GSC)	Further elaborate on the concept of execution context.
April 2014	1.3	Global Standards Council (GSC)	Added section 3.4.5 on adaptor and connector architectural options.

Editors

Scott Came	James Douglas	David Gillespie
John Ruegg		

Note: If any users have difficulty accessing these materials due to a disability they may have, please contact Global at Global@iir.com for assistance in receiving an alternative format.

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.