WHITEPAPER

ASTCORPORATION

Adopting Global Standards for Justice Information Sharing:

Part One – The GRA

Daniel DiMarco

October 2016

AST CORPORATION

CONTENTS

1 ABSTRACT

Integrated justice information systems are critical for accurate, timely, and informed decision-making. Law enforcement, courts, and corrections need to communicate in a seamless, secure manner to efficiently manage the criminal justice process and maintain order for all citizens.

Unfortunately, agencies with vast amounts of data and heterogeneous technologies that attempt to share information across departments and between partners struggle with **complexities**, **costs**, and **compliance.**

To help overcome these difficulties, the U.S. Department of Justice recommends (or requires for federal funding) standardization. The best-practices approach, designed to reduce implementation time and costs by 80 percent, is known as the Global Reference Architecture, or GRA.

The GRA is a service-oriented approach for justice and public safety information sharing. It is part of the Global Standards Package that includes the National Information Exchange Model (NIEM) and the Global Federated Identity and Privilege Management (GFIPM) program. The use of these standards is important to lower overall acquisition costs and enhance data messaging and systems integration across justice agencies.

This is the first of a two-part paper that explores the details of the GRA flexible blueprint and its components.

2 ACRONYMS AND DEFINITIONS

Acronym	Definition
BJA	Bureau of Justice Assistance
BPEL	Business Process Execution Language
CJA	Criminal Justice Agency
CJI	Criminal Justice Information
CJIS	Criminal Justice Information Services
GFIPM	Global Federated Identity and Privilege Management
GRA	Global Reference Architecture
GSC	Global Standards Council
GSP	Global Standards Package
JAG	Justice Assistance Grants
JPS	Justice & Public Safety
IEPD	Information Exchange Package Documentation
NIEM	National Information Exchange Model
OSI	Open System Interconnection
SIP	Service Interaction Profile
SOA	Service-Oriented Architecture

3 INTRODUCTION

The need for Justice and Public Safety (JPS) agencies to manage mission-critical information across boundaries has intensified due to both an influx of sensitive data and an uptick in global disorder.

Faced with a myriad of data/application management challenges and oftentimes aging technologies, JPS organizations are turning to the Department of Justice standards to guide them through a software upgrade process and to the appropriate level of preparedness.

The need for Criminal Justice Information Services (CJIS) systems, guided by the Global Standards Council, is quickly rising.

4 GLOBAL STANDARDS PACKAGE

Built on the cornerstones of interoperability, sustainability, and cost-effectiveness, the Global Standards Council (GSC) is responsible for the development and maintenance of normative technical standards for justice information sharing. To achieve these goals across the justice and public safety community, as well as consistency and standardization, the GSC developed the Global Standards Package (GSP).

The three primary components of the GSP are:

- Global Reference Architecture – GRA
- Global Federated Identity and Privilege Management – GFIPM
- National Information Exchange Model - NIEM*

JPS agencies have long embraced the GSP as the best-practices approach to building efficient, integrated justice systems. Now there is a growing need for robust vendor-neutral systems that can manage and store data, easily integrate, and meet security requirements.

Furthermore, the Criminal Justice Agencies (CJAs) responsible for dispersing Byrne Justice Assistance Grants (JAG) now require agencies to comply with GSP standards to be eligible to receive funding for information sharing.[1]

[1] Roshan Parab from AST Corporation has written a helpful paper on the National Information Exchange Model (NIEM), which can found at: http://www.astcorporation.com/whitepapers.html.

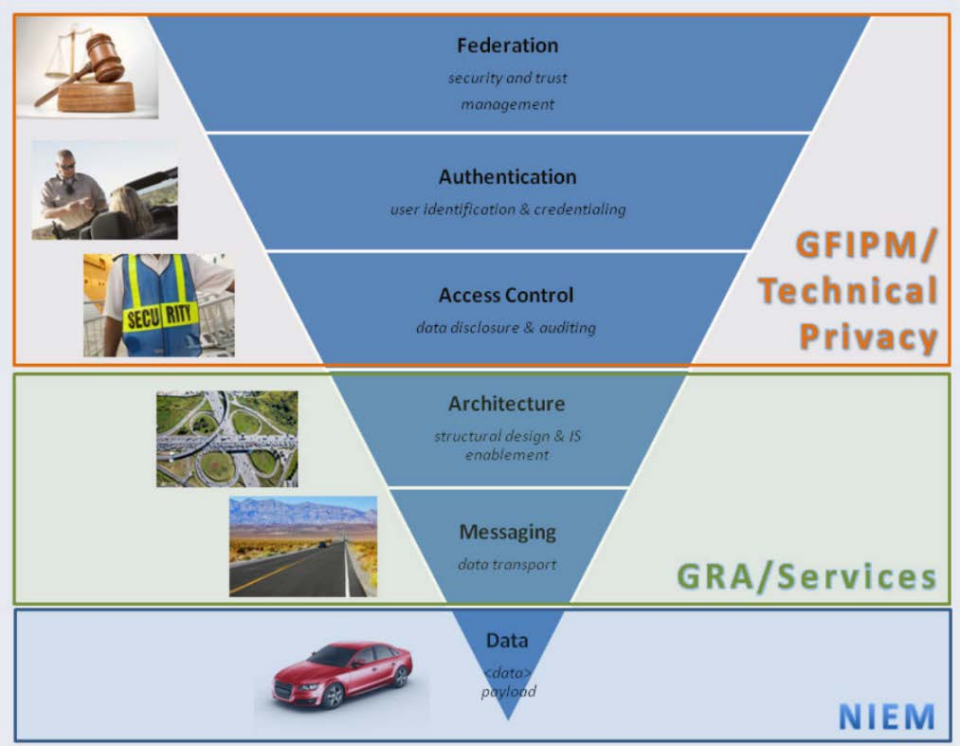

Figure 1 The GRA is often used to bridge the secure, encrypted transfer of the preferred common data format that is NIEM; Organizations frequently turn to the GSP toolkit when developing and deploying CJIS systems.

Recently, a number of states have made a significant push to adopt the standards and implement baseline requirements for the management and security of Criminal Justice Information (CJI). The recent strides made in the information sharing mission for the Justice & Public Safety (JPS) community can be attributed to a combination of factors:

- A dedicated effort led by state CJAs as they look to extend the benefits of justice information sharing;
- Technologies that inherently possess the core components to achieve data management, security, and standardization goals;
- The growing skillset of IT professionals capable of implementing, integrating, and managing the systems; and
- The GSP roadmap and toolkit led by the Global Reference Architecture – GRA.

5 GRA – Global Reference Architecture

GRA is an abstract framework for understanding significant components, and the relationships between them, within a Service-Oriented Architecture (SOA). It lays out common concepts and definitions as the foundation for the development of consistent SOA implementations within justice and public safety communities.[2]

The GRA was developed by the Global Infrastructure and Standards Working Group, a collection of public sector, nonprofit, and private industry SOA experts.

The two main objectives of the GRA are to speed agency adoption of SOA-based approaches through its framework and to offer a standard methodology for creating services that align with business functions. Consequently, conformance generally relies on adherence to at least one of these paths.

Service-Oriented

Although somewhat technical in nature, SOA can be broken down into three key areas.

1. Modular or Insulated Layers of Technology: Creating a service layer that is independent makes that service easier to reuse or modify. The decoupled nature of the layer makes it flexible and scalable, ideal for data exchanges.
2. Open Standards: SOA-based information sharing is all about open participation and is not reliant on specific or proprietary technology.
3. Formal Governance: A SOA roadmap defining and coordinating policies, decision-makers, and business processes is paramount to success.

The increased agility achieved with SOA methods and principles has made it a popular route for integration among many organizations, across industry verticals.

[2] Source: BJA - Global Reference Architecture, Framework, Version 1.9.1

Reference Architecture

A set of documents that can be used to reference a project is another important component of the GRA. Various tools can be used to design visual models and create clear viewpoints for participants to follow and add to. This helps promote consistent thinking across the disparate systems and multiple boundaries that are often involved with JPS information exchanges.

Service Identification

In order to achieve long-term information sharing goals, an organization needs to identify and utilize certain business-oriented methodologies. When identifying services and the priorities given to their deployment, a combination of the following common approaches is recommended by the GRA:

- Business functions
- Goal-driven
- Existing supply
- Front office usage analysis

It is also important to document a business capabilities analysis. This becomes a catalog of service candidates that is created based on valuable current systems, interfaces/applications, and what future capabilities should be prioritized to provide enhanced value. These steps, and more, can be followed using the Global Reference Architecture Service Identification and Design Document.

Infrastructure Recommendations

The GRA does not dictate which equipment and software to purchase or vendors to use, but its Execution Context Guidelines elaborate on many of the details for a successful implementation.

6 EXECUTION CONTEXT GUIDELINES

Execution Context is a critical set of infrastructure elements, processes, policy assertions, and agreements that form a secure communication path between the consumer of a service and the service, which provides access to the capability that can meet the consumer needs. Common shared elements throughout an infrastructure make up a shared execution context and are the focus of SOA implementers looking to share multiple contexts for numerous service deployments.

Implementation guidelines are organized into four areas:

- Reachability
- Willingness
- Awareness
- Intermediaries

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."

It is important that network infrastructure provide a physical path with conformant components to allow service participants to share information. Examples of GRA conformant network communications components that support Reachability are:

- Wide Area Network – WAN;
- Local Area Network – LAN;
- Internet; and
- Wireless networks.

A Service Interaction Profile (SIP) is also necessary to define the messaging capabilities of the infrastructure. This should consist of:

- Service interaction requirements;
- Interface description requirements;
- Message exchange patterns; and

- Message definition mechanisms.

This ensures that various messaging protocols in use by any providers or consumers of services can be supported by the message transport infrastructure.

The following table[3] provides the guidelines to apply the Open System Interconnection (OSI) Reference Model to the infrastructure to support the reachability.

OSI Layers	Layers 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. Global Reference Architecture
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. National Information Exchange Model
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 SIPs.
6	Presentation	
7	Application	

[3] Source: BJA – Global Reference Architecture, Execution Context Guidelines, Version 1.3

Willingness

The concept of Willingness within the GRA relates to the overview of how a service provider and service consumer interact.

There are five target areas of conformance to GRA guidelines for the Willingness of shared infrastructure.

Network infrastructure security[4]

1. Firewalls
2. Virtual private networks (VPNs)
3. Secure sockets layer (SSL)
4. Attack detection and prevention
   - XML security devices/firewalls
   - Intrusion detection system (IDS)
   - Virus detection systems
5. Security auditing
6. Risk management
7. Disaster recovery and business continuity

Wireless network infrastructure security—Expertise in the deployment of firewalls, VPNs, and virus-protection is necessary to ensure the proper mitigation of risks in a wireless environment.

User/system/service identity provisioning and management

1. Directory services—Lightweight Directory Access Protocol (LDAP) and other open standards should be considered when implementing directory services.
2. Identity management—Integrate with directory services for shared support across multiple applications, systems, and services.
3. Federal Identity and Privilege Management – Federated identity concept.
4. Public key infrastructure (PKI)—Supports confidentiality, nonrepudiation, and message integrity functions.

[4] Note: Security and privacy will be covered in Part 2 of this whitepaper - GFIPM

Shared security infrastructure ("authentication")

1. Authentication
2. Coarse-grained authorization

Security policy infrastructure ("authorization")

3. Fine-grained authorization
4. Authorization policy
5. Policy Decision Point (PDP)
6. Policy Enforcement Point (PEP)
7. XML Access Control Markup Language (XACML)
   - OASIS XML-based Policy Assertion Language (PAL)
8. Policy authoring tools

Awareness

Service registries and repositories provide the capability for owners, designers, and implementers to thoroughly understand a service's behavior and information. Infrastructure that supports Awareness should have a query function that facilitates the discovery and retrieval of artifacts.

Repository infrastructure should also consider providing the following capabilities:

- Submission, approval, deprecation, and deletion of content;
- Content management of metadata;
- Security;
- Auditing;
- Event notification; and
- Federated registry.

Intermediaries

The connections that mediate the exchange of information between consumers and providers are called intermediaries. Made up of connectors (consumer side) and adaptors (provider side), these key SOA components ensure separation of the integration

logic from the complexities of the partner systems for high reusability with loosely coupled services.

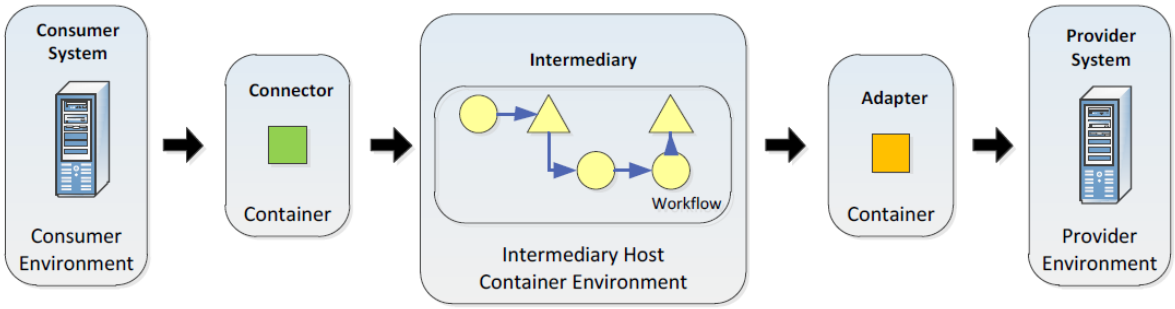

Figure 2 Source: BJA – Global Reference Architecture, Execution Context Guidelines, Version 1.3

One of the benefits when implementing a GRA/SOA-based data exchange is avoiding the costly and inflexible alternative of point-to-point integrations. Experienced systems integration architects and SOA developers play a critical role in successful results.

Other Intermediaries

Message Routers: Based on rules applied to the context of the message, routers receive messages, examine them, and then transmit them to the proper place. Here again, GRA conformance is based on the support and definition of the components that perform the task.

Orchestration: Coordinating interaction with multiple services, orchestration is a highly useful technique to compose hierarchical, service-oriented business processes. This should be performed according to the best practices outlined by BPEL – Business Process Execution Language. The GRA requires conformance to BPEL guidelines, with messaging infrastructure that supports:

- Deployment;
- Management;
- Maintenance; and
- Execution.

Transformers: Services that receive a message and transform it to another format before transmitting it to its next destination.

Message Validators: Message inspectors looking for conformance to business rules, message requirements, and service specifications.

Interceptors: Capture information for analytics and reporting purposes.

Security Token Services: Services that accommodate a variety of authentication and authorization mechanisms.

7 OTHER OPERATIONAL CONSIDERATIONS

Guidelines for non-operational infrastructure are not explicitly stated as part of GRA conformance, but recommendations of quality and assurance are in place for:

- Performance;
- Availability;
- Maintenance; and
- Scalability.

8 SERVICE SPECIFICATION PACKAGE

In order to achieve conformance targets, a Service Specification Package (SSP) should be assembled. The SSP is portable, self-contained, and self-documented. It provides a consistent model for documenting GRA services.[5]

The Service Specification Guidelines (SSG) identify the following conformance targets for the SSP.

- SERVICE DESCRIPTION
- SERVICE INTERFACE DESCRIPTION
- SERVICE METADATA
- SERVICE CATALOG
- SERVICE SPECIFICATION CHANGE LOG
- SERVICE SPECIFICATION INFORMATION MODEL
- SERVICE SPECIFICATION BEHAVIOR MODEL
- SERVICE SPECIFICATION SCHEMAS
- SERVICE SPECIFICATION SAMPLES
- SERVICE SPECIFICATION PACKAGE

Similar to NIEM IEPDs that describe the conceptual, logical, and physical models of data, the SSP describes a service. Also in similarity, the complete packaging process produces a clear view of capabilities and requirements.

[5] Source: BJA, GRA, Service Specification Package, Version 1.2.0

9 GRA Guidelines as a Key Risk Management Tool for JPS

Body-worn cameras, Case/Jail Management systems, and disparate cloud and on-premises technologies all pose significant data and integration challenges to JPS organizations.

The GRA policy and governance that helps establish and monitor a SOA framework is imperative for the critical sharing, auditing, monitoring, and managing of data, applications, and processes. The benefits of the GRA highlighted throughout this paper – reusability, flexibility, scalability, extensibility…all help mitigate a multitude of risks. The standardized framework becomes an organization's first line of defense against the growing cascade of JPS data and heterogeneous technologies.

10 LEARN MORE

Additional technical assistance and advice can be found through the following Bureau of Justice Assistance partners:

- Integrated Justice Information Services Institute – IJIS - www.ijis.org
- National Center for State Courts – NCSC - www.ncsconline.org
- National Consortium for Justice Information and Statistics – SEARCH - www.search.org

11 SUMMARY

When properly implemented by a skilled SOA architect, a GRA infrastructure is the ideal foundation for the sharing of accurate and timely mission-critical information, reducing complexities and risk along the way.

Organizations that follow the GRA roadmap will have maximum access to federal funds for justice information sharing, and the flexibility needed to manage a multitude of future JPS challenges.

Coming Soon – Part Two: Global Federated Identity and Privilege Management – GFIPM

About the Author:

Daniel DiMarco

Daniel DiMarco is a Senior Consultant with over 23 years of Risk and Project Management experience. As a professional in the financial industry, he collected and correlated public and private sector data, aggregating it for improved decision-making. He has been involved in the evaluation of various U.S. and International government statistics, and also studied the efficiencies of supply chain conglomerates. Mr. DiMarco specializes in research, documentation, and contingency planning.

Prior to AST, Mr. DiMarco held a consultant position for a company performing ERP integration, working with Oracle's JD Edwards. There, he assisted IT leadership in business process automation for manufacturing and education.

Currently, Mr. DiMarco is an integral part of AST's Justice and Public Safety Practice, helping JPS agencies implement Global Standards and CJIS systems while undergoing a measured migration to newer technologies.

Adopting Global Standards for Justice Information Sharing:
Part One – The GRA
October 2016

Specialized. Recognized. Preferred. The right partner makes all the difference.

AST Corporation is a privately held company, founded in 1995, to serve commercial and public sector organizations in utilizing the full potential of their investments in Oracle Applications. We have built our business by providing top quality full life cycle and turn-key consulting services for Oracle implementation and upgrade projects, among other specific services.

Our mission is to ensure that you, as a valued client, receive the highest level of expertise and personalized service for your Enterprise Applications. We endeavor to help you realize the full benefit from your investment in software applications and integrate them seamlessly to your business processes.

AST CORPORATION

AST Corporation
1755 Park Street, Suite 100
Naperville, Illinois 60563

Phone: 888-278-0002
Fax: 630-778-1179
www.astcorporation.com