Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle’s products remains at the sole discretion of Oracle.
Document Scope
This paper gives readers an overview of Oracle’s approach to providing a robust and feature-rich platform upon which to develop, deploy, and manage NIEM-based information exchanges. NIEM is an abbreviation for National Information Exchange Model, and NIEM is at the core of the government’s efforts to standardize information exchange among all levels of government. This document covers the following topics:

1. Business Drivers for Information Exchange
2. NIEM Overview
3. Oracle Reference Architecture
4. Summary

Business Drivers for Information Exchange

Increasingly, government organizations need to exchange data with other agencies and jurisdictions as a way to meet the growing demands for information exchange. This includes all levels of government, both horizontally (state to state) and vertically (local to state or state to federal). The two government verticals where this is most urgent are in justice and public safety (JPS) as well as health and human services (HHS). In JPS, the business drivers for information exchange are:

1. Exchanging criminal data such as bookings, warrants, and CJIS (Courts/Justice Information Systems) information
2. Exchanging suspicious activity reporting data (referred to as SAR data)
3. Exchanging gang-related data
4. Exchanging alerts, notifications, and situational awareness information
5. Emergency preparedness information

In contrast, the business drivers for HHS information exchange are largely due to the Affordable Care Act of 2010:

1. Health Information Exchange
2. Health Insurance Exchange
3. Medicaid modernization and expansion
4. Integrated eligibility and enrollment

As a result of these emerging business drivers, the U.S. government quickly realized that they needed to establish standards and frameworks to facilitate intergovernmental information exchange. The first framework they developed was NIEM, and NIEM is focused standardizing
the contents of the data message being exchanged. However, there are other
frameworks/standards that are highly interrelated to NIEM. The following section details NIEM
and these other standards.

**NIEM Overview**

At its core, NIEM is a framework (created by the U.S. Department of Justice and Department of
Homeland Security) designed to facilitate information exchange between various government
organizations at all levels (federal, state, and local). However, more broadly, NIEM is part of a
family of frameworks and standards put forth by the federal government, including

1. National Information Exchange Model (NIEM)
2. Justice Reference Architecture (JRA)
3. Global Federated Identity and Privilege Management (GFIPM)

These frameworks and standards greatly facilitate reuse, interoperability, security, and reliability
with regards to implementing an information exchange. More specifically, NIEM defines a
framework for defining and reusing XML schema definitions such that government
organizations can use a common language when exchanging data. NIEM also defines numerous
domains based on the type of government function (such as emergency management, justice, or
health). Within these domains, exchange developers are encouraged to reuse, extend, and
contribute various message definition files called Information Exchange Package Definitions
(IEPDs) to the NIEM community. In addition, NIEM has evolved such that government
architects have defined the JRA. JRA provides numerous guidelines, best practices, and NIEM-
related standards such as

1. Reference architecture planning information
2. Service specification packages
3. Technical implementation guidance
4. Policy guidance

JRA leverages SOA and Web services standards (as defined by OASIS) as a foundation for their
architecture, and then provides additional prescriptive guidance on how to leverage and best
implement these standards.

Finally, the federal government has defined a security standard to facilitate interoperability,
courage the use of best practices, and shorten project schedules. This standard is called Global
Federated Identity and Privilege Management (GFIPM). Specifically, GFIPM was created to
standardize how exchanges secured their environment, focusing on

1. Authentication of users
2. Encryption of data to maintain privacy
3. Authorization based on user attributes and the context of the request

In order to meet these requirements, GFIPM uses the following foundational standards:

1. Web Services Security
2. WS-I Basic Security Profile
3. SAML-based authentication
4. SAML-based attribute assertions
5. XACML-based authorization

More specifically, there are several key components to a GFIPM-based infrastructure that should be considered:

1. Browser-based security federation (such as via WS-Federation and SAML)
2. End-user attribute aggregation and communication
3. Token mapping
4. Request/message authentication, integrity, and non-repudiation
5. Service authorization

The following picture illustrates these requirements and associated components:

**Figure 1. GFIPM Exchange Security**

The picture above illustrates the potentially complex environment in which an exchange must operate. One of the challenges in this environment is converting from one set of security...
credentials ("tokens") to the GFIPM standard using SAML and supporting GFIPM user attributes. In addition, users may be coming in via their own existing user interface or via an exchange-specific portal; in either case, the user credentials need to be captured somehow. Finally, one must query an authorization service to determine whether the user should be granted access. What follows is a description of the Oracle reference architecture that supports NIEM, JRA, and GFIPM. This reference architecture is based on a Service-Oriented Architecture (SOA) approach, and it can be used in most any context where these types of requirements exist.

Oracle’s Reference Architecture for NIEM Exchanges

Oracle offers a comprehensive solution for implementing NIEM-based information exchanges. Our approach offers four key things:

1. Robust, enterprise-grade infrastructure software
2. Comprehensive approach addressing all your exchange needs
3. Pre-integrated middleware products and state-of-the-art tools
4. Knowledge and experience in designing NIEM-based exchanges

In addition, Oracle is very active in the NIEM and standards-setting communities. What follows is a pictorial representation of Oracle’s reference architecture for NIEM.

Oracle Reference Architecture

The following section details each of these solution areas and describes the components within.
Oracle Identity and Access Management Suite

Oracle’s Identity and Access Management Suite (OIAM) offers comprehensive security aimed at organizations with a heterogeneous environment. OIAM provides the following features/services:

1. Adaptive end-user authentication with fraud detection
2. Single sign-on to integrate user access on the front-end
3. Coarse-grained access control based on role
4. Self-service password reset
5. Automated provisioning of users and their privileges
6. Role management
7. Credential/token mapping
8. Fine-grained authorization
9. Security policy management
10. Encryption
11. Auditing and attestation support

This includes extensive support for standards, as well as “security as a service” support throughout the product line. Supported standards include: SAML, XACML, SPML, WS Security, WS Federation, X.509, and so on.

Oracle WebCenter Suite

Oracle WebCenter provides a powerful user interface and collaboration platform on which to deploy your user-facing applications. WebCenter provides browser-based thin-client access to your enterprise applications via extensive support for Web-based clients, including multichannel access via mobile devices. WebCenter is a unique offering in that it blends complete support for all of the following:

1. Traditional portal platforms
2. Composite applications
3. Social/collaboration interfaces
4. Content and document management

More specifically, the following list summarizes the major features provided by WebCenter:

1. User interface design tool with customizable layouts and styles
2. Collaboration services such as wiki, blog, document management, discussions, notifications, task management, email, and so on
3. Personalized interfaces based on user role
4. Business activity streams whereby users easily navigate and discover relevant content
5. Dynamic “spaces” where users can join groups, sharing documents and other information in a secure manner
6. Rich library of user interface components for UI/portal developers
7. Delegated administration capability for large or federated organizations
8. Real-time and intelligent collaboration; messaging and content application where users discover and communicate information based on context and properties

Oracle SOA / BPM Suite

Oracle SOA Suite is a SOA-enablement platform that provides organizations with a robust infrastructure to support application integration, service orchestration, business process management, and messaging. Business Process Management (BPM) capability with human workflow support can be purchased as an add-on to the SOA Suite. The major features of SOA/BPM Suite are:

1. Design time and runtime environment for automating business processes and integrating disparate applications and external connections
2. Support for multiple protocols and data formats via an enterprise service bus (ESB)
3. Tool-generated data transformations to/from flat files, binary, and XML
4. Business Activity Monitoring (BAM) dashboards for business managers and IT managers to track processes and activities flowing through the SOA/BPM Suite
5. Human workflow support including support for industry standards such as BPMN and BPEL
6. Complex event processing (CEP) to support automatically aggregating, correlating, and alerting multiple events over some specific time period (very useful in JPS and HHS). Use-case examples include correlating criminal, gang, or terrorist events in JPS, and correlating prescription drug monitoring events in HHS. CEP is a clear differentiator for Oracle, giving our customers the power to perform real-time and sophisticated event aggregation and correlation while keeping this relatively simple and cost-effective by embedding CEP into our SOA Suite. We offer the unique ability to do this without human intervention, and in concert with real-time message/transaction activity as well as leveraging existing database data.
7. Business rules support for making intelligent decisions with respect to routing, service orchestration, or business process flows
8. Comprehensive security support for authenticating, authorizing, and encrypting/decrypting users and data as they flow through the system
Oracle Governance

Oracle’s Governance solutions include comprehensive support for managing your SOA-related artifacts. This includes the full lifecycle from approving newly-designed artifacts to deployment to automated discovery and management of artifacts such as Web services, business components, security policies, schema files, and so on. These preintegrated governance products include:

1. **Oracle Enterprise Repository**: Save project artifacts and make it easy to report on dependencies and usage
2. **Oracle Service Registry**: Keep a real-time catalogue of services and their properties to better manage your SOA environment
3. **Oracle SOA Management Pack**: Start, stop, debug, test, and manage your SOA environment in Oracle’s integrated enterprise management console

Oracle Audit Vault

Oracle Audit Vault provides a centralized, secure, and reliable repository for your audit data. Auditing has evolved to be more than a best practice, and is essentially a mandated business activity in today’s IT environment. Our Audit Vault provides the following:

1. Ability to collect and monitor data from multiple disparate sources
2. OOTB compliance and entitlements reporting
3. Alert notifications
4. Open and extensible design

Oracle Database with Security Options

One of Oracle’s major differentiators is the extensive security features available in the database product. Oracle offers many features out of the box and many more as add-on options. Here is a summary of some of these.

1. **Advanced Security Option**: Supports transparent encryption of key data (such as PII/PHI)
2. **Fine-Grained Auditing**: Create audit policies with detailed control over how/when an audit record is generated
3. **Enterprise User Security**: Secures DB users with provisioning and role-based access controls and password management
4. **Data Vault**: Provides greater control (including DBA control) over how/when data can be accessed, including segregation of duties support

Oracle Data Integration Suite

Oracle’s Data Integrate Suite offers the following best-of-breed data management capabilities:
1. Aggregate, cleanse, and transform large sets of data
2. Change-data capture between heterogeneous and legacy systems
3. Service-enabling data management tasks including exposing these tasks as Web services
4. Real-time data replication among disparate and remote systems

NIEM Tooling

There are many tools available to design NIEM messages. Oracle offers a best-practice approach to designing your NIEM exchange messages, leveraging a combination of online tools and free development tools. Specifically, we currently recommend the following approach:

1. Leverage Subset Generator Tool (SSGT) to “shop” for IEPD artifacts and particular elements of interest within existing domain IEPDs. (An IEPD is a package of documents that facilitates reuse of schemas across projects and among various NIEM domains.)

2. Once you have chosen your base schemas, use the CAM tool to import the schemas, and then generate a reusable template that facilitates making changes. CAM is a freely available open-source tool that has been adopted as an OASIS standard. CAM greatly facilitates iterative, round-trip design/engineering of your schema files, so we recommend using CAM rather than SSGT for this step. Moreover, CAM includes “dictionaries” for almost all the NIEM domains and elements, and you can create and extend your own dictionaries. These dictionaries give CAM the ability to simplify and streamline the NIEM message design process. Also note that these dictionaries adhere to the UN/CEFACT ISO 15000-5 CCTS standard.

3. Use CAM to check for NIEM conformance. CAM identifies violations of the NIEM naming and design rules (NDR), and scores the schema on percentage of conformance.

4. Use CAM to export the final schema files into a directory, and you can then leverage these schemas for any Oracle-related projects, such as using Oracle SOA Suite to implement your exchange.

Finally, note that CAM is being enhanced to include support for drag-drop and search, so this will provide an alternative to SSGT with regard to step 1 above. More tool-related information is available at the following Web sites:

http://tools.niem.gov
http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cam
Conclusion

As described herein, Oracle provides a very comprehensive and feature-rich platform on which to build a SOA-based information exchange. In addition, each product has been pre-integrated to work well with the other components, providing numerous cross-product features for installation, design, and management. Oracle also invests heavily in industry standards as a way to offer customers choice rather than vendor lock-in. In summary, Oracle’s strength is in providing best-of-breed solutions that are easy to install, configure, design, deploy, and manage. We like to think of our platform as the “foundation for agility” while also lowering long-term costs and allowing organizations to focus on their business objectives.