Justice Information Exchange Model

Conceptual Framework

**SEARCH--The National Consortium
for Justice Information and Statistics**

Justice Information Exchange Model: Conceptual Framework

SEARCH--The National Consortium for Justice Information and Statistics

Copyright © 2008-2010 SEARCH Group, Inc.

Table of Contents

JIEM Conceptual Framework

The Justice Information Exchange Model (JIEM) consists of four components:

- A conceptual framework for understanding information exchange between business partners and their systems (this document)

- A methodology for analyzing current information exchange and for reengineering information exchange in an integrated business environment

- The JIEM Modeling Tool, a software package to assist practitioners in applying the model to their site

- JIEM Reference Models, a set of information exchanges common to most jurisdictions in a particular domain

The conceptual framework for understanding information exchange, simply stated, it is that for most business domains (including justice, public safety, homeland security, etc.), all information exchange can be described in five dimensions: process, event, agency, condition, and information. The information dimension includes documents and their structure (data containers, data elements, data types, and associations).

JIEM users create models of the information exchange requirements in their jurisdiction or environment. Such a model is called a *Site Model*. In version 4.0 and higher of the JIEM modeling tool, a site model is a simple XML file containing information from each of the JIEM dimensions.

JIEM Dimensions

Process

A Process is a group of logically related events that trigger and follow after information exchange. There are two processes associated with an information exchange, a Prevailing Process (the business process in which the Triggering Event occurs), and a Subsequent Process (the business process in which the Subsequent Event occurs). Processes have the following characteristics:

- They extend over time.

- They begin and end with an event.

- They may contain multiple events.

Processes may also exist concurrently with other processes. For example, in the justice domain, a subject may be detained while being tried, and exchanges in both the Detention and the Pre-disposition Court processes may occur at the same time.

Processes may also exist consecutively with other processes. For example, in the justice domain, the Pre-disposition Court process ends where the Post-disposition Court process begins.

Event

There are two kinds of events associated with an information exchange, triggering events and subsequent events. The Triggering Event is a decision or action that causes the exchange of information. The Subsequent Event is the next logical step in the business process that results from the information exchange. Very often the Subsequent Event is a Triggering Event for yet another information exchange.

For instance, in the justice domain, a Prosecution Charging Decision occurs when the prosecutor reviews law enforcement charges and determines whether to file an official charging document with the court or to reject prosecution. Similarly, a Court Appearance is an action by the court that also leads to information exchange in the justice system. Similarly, when the prosecutor files charges with the court, the court accepts charges and schedules a court event. The calendaring of the court event triggers communication of that scheduling information, which constitutes additional information exchange.

There are occasions when an agency receives information and takes no action that results in information exchange. For example, one business partner may send a message to another, and upon receipt the sending agency generates a paper document and places it in its case file. When this occurs, the Subsequent Event describes an internal activity - updating the case file - rather than a Triggering Event.

Events have the following characteristics:

- When used as Triggering Events, they are the primary reason for the information exchange.

- They represent an activity that is instantaneous or a slice in time (occurs in an instant, within several hours, or within several days at the most).

Agency

An agency in JIEM is a business organization within an information sharing enterprise that either provides information to other agencies, consumes information from other agencies, or both. An agency can be

any subdivision or sub-unit of a larger enterprise (such as a county or state government) that owns or controls information or the technology assets (systems) that manage that information. The term "agency" is applied generically to branches of government, divisions, departments, and all other organizational units, and sometimes to major functions within an organization.

Each exchange in JIEM includes one or more Sending Agencies and one or more Receiving Agencies.

Examples of agencies in the justice domain are: Law Enforcement, Prosecutor, Defense, Court. These entities include traditional justice agencies, as well as justice-related organizations (i.e., diversion provider, mental health, social services) that send or receive information in paper, electronic or other forms as part of the justice process. In addition, the JIEM Adult Felony Reference Model 1.0.1 divides the traditional functions of a sheriff's office into three agency identifiers: law enforcement, for duties similar to those performed by police departments; jail, for detention and incarceration functions; and sheriff, for warrant and service of process activities.

The JIEM Adult Felony Reference Model also identifies generic activities that may be housed in different agencies from state to state. For example, collection of fines, fees, costs, and restitution may be performed by the court in one location, by the prosecutor in another, and probation in another. In the reference model, Collecting Agency is the designation for this activity, but JIEM users are free to assign this responsibility to whichever local organization is appropriate.

Conditions

A condition is a factor that affects the content or direction of the information exchange. Multiple exchanges may be spawned by a single triggering event; it is the combination of conditions that determines which exchanges occur.

Conditions have the following characteristics:

- Conditions may help to determine who gets what.

- Conditions must be true for a particular exchange to occur.

- Absence of a condition is acceptable in the model, but is not allowed by the software.

- Conditions have a subject and a predicate and usually refer to a decision, action, situation, or state of being.

Each condition must contain a subject and a predicate, and the model should not represent the condition in the passive voice. In other words, the condition must specify who is taking the action or making the decision. The only exceptions are when the condition defines that state of a person or object (e.g., if subject is an adult), or the expression of the condition is overly complex or vague if stated in the active voice ("if law enforcement, court, probation, parole, or other justice organization captures subject" is stated as "if subject is captured").

Information

Information is defined as the actual data that is exchanged between the sending and receiving agencies. It includes documents - paper, electronic, or other forms of communication. A single information exchange may include multiple documents, but must contain at least one. For example, in the justice domain, when a law enforcement agency forwards a case to the Prosecutor for the Prosecution Charging Decision, it may send an Arrest Report and an Offender Tracking Form. All documents associated with a single transfer decision should be included in the exchange.

A document type is associated with each JIEM document. In the current version of the JRM there are two document types, paper and electronic. Future versions of the model may contain additional document types.

Documents consist of a prose description and a formally-represented definition of the document structure. In JIEM, Documents and their underlying structure together represent the *Information Dimension*, and the information about them is captured in an Information Dimension Model. [1]

Each document in JIEM can contain one or more Data Containers. A Data Container is a representation of some person, place, or thing in the real world (a noun). A Data Container contains Data Elements and Associations. A Data Element is a single-valued attribute of the object represented by the data container. For example, "city" and "state" might be Data Elements within an Address Data Container. Each Data Element has a Data Type; Data Types can be "standard" (such as strings, numbers, and so on) or they can be user-defined (such as lists of codes or specialized restrictions of strings or numbers). Associations represent named links to other data containers, and reflect a relationship between objects. For instance, a Person data container may have an association to an Address data container, representing the fact that a Person lives at an Address.

Data Elements and Associations can be assigned cardinality, to indicate quantities. For example, the information dimension model may specify that a Person can have one or more (1..*) Addresses. A cardinality of zero or more (0..*) means a data element or association is "optional"; a cardinality of one to one (1..1) means a data element or association is "mandatory" but can only exist once.

Data containers can also exist in a "specialization" relationship with other data containers. When one real-world object is a special kind of another (e.g., an Automobile is a special kind of Vehicle), the data container representing the one object can extend the data container representing the other. This allows the model to reflect the semantics of specialization, and also aligns the model with industry standards such as UML and XML Schema.

The JIEM Information Dimension allows Documents to share data containers. It accomplishes this by providing a "shared components" area that contains Packages; each Package can contain one or more data containers (and the data elements and associations contained within them) for reuse across documents. JIEM also allows users to leverage content defined in XML-based standards, such as the National Information Exchange Model (NIEM); "shared components" area for storing data containers derived from these standards. Shared components encourage good modeling practices by promoting component reuse and leveraging of established national standards.

The JIEM Information Dimension is compatible with NIEM concepts including; Global Data Elements, Enumerations, Document Root Elements and utilizing Wantlists. Insuring that the JIEM Information Dimension is compatible with NIEM concepts allows tools to develop the ability to export NIEM compliant Information Exchange Package Documents (IEPD).

It is useful to think of documents (and their structure) captured in JIEM as "prototype documents" for exchanges.

---

[1]Versions 4.0 and earlier of the JIEM software captured data elements in a simple structure that did not differentiate between elements and their types. This created difficulty for mapping JIEM documents to Information Exchange Package Documentation (IEPDs), in particular IEPD exchange content models created in UML. Version 4.1 of the JIEM software allows users to create document structures in UML, via a simplified, user-friendly editor.

JIEM Exchanges

An Exchange in JIEM brings together all the other dimensions (Process, Event, Agency, Condition, and Information) and represents an actual instance of information sharing between business partners. Exchanges represent the lifeblood of criminal justice, public safety, intelligence, homeland security, and other public sector business domains: the sharing of mission-critical information between autonomous but collaborating organizations within the same enterprise. Exchanges may manifest in the sending/receiving of paper documents, batch file transfers, inter-system message exchanges, shared database transactions, or other technological approaches. The important aspect of the Exchange dimension in JIEM is that it reflects the business requirements around these technology implementations.

Each exchange identifies:

- One or more sending agencies

- One or more receiving agencies

- The prevailing process

- The subsequent process

- The triggering event

- The subsequent event

- Conditions under which the exchange takes place

- Documents (and a link to the structure of the documents) representing the information being exchanged

Additional global variables are used to describe exchanges, and users can add local variables of their choosing to their site models. The global variables are as follows:

- *Frequency:* the average number of times per month this exchange is estimated to occur.

- *Urgency:* the speed at which the information is needed by the receiving agency.

- *Priority:* the importance of automating this exchange in an integrated justice initiative.

- *Complexity:* the relative difficulty or cost of automating this exchange.

- *Duration:* the average length of time currently required to complete this exchange.

- *Transaction Type:* the type of exchange, such as a query/response, push/pull, publish, or subscribe/notify.

- *Perspective:* this exchange describes the current "As-Is" system, the desired "To-Be" system, or both.

- *Status:* work on this exchange is in progress or complete.

- *Confidentiality:* this exchange is public, confidential, or private.

- *Location:* used when the business rules or information flow vary from location to location within a jurisdiction.

- *Additional Business Rules:* used to document additional factors that are important to understand the context of an information exchange.

- *Notes:* used to capture notes that are important to allow business partners to understand more about the information exchange.

In addition to these global variables an exchange can have performance measures and policies associated with it.

JIEM Policies

A policy is a set of rules or statements that define appropriate actions in a particular scenario. In the context of justice information exchange, policies describe the conditions in which specific information can be collected, shared, or withheld. Policies perform two essential purposes;

1) establishes public trust through transparency, and

2) clearly articulates compliance with established laws, regulations, and/or administrative rules.

Information exchange polices are nothing new to the justice community, as a myriad of laws, regulations, and administrative rules currently exist that govern the conditions for public access, protecting an individual's privacy, and withholding sensitive or investigative information.

JIEM includes a feature to assist justice practitioners implement electronic privacy and access control policies within the context of information exchange. Under the direction of the JIEM Steering Committee and with the support of the U.S Department of Justice Bureau of Justice Assistance, SEARCH leveraged the guidelines described in the document titled 'Implementing Privacy Policy in a Justice Information Sharing: A Technical Framework', which was authored by the Global Security Working Group Technical Privacy Task Team. This document (referred to as the Tech Framework) builds upon previous Global privacy policy work products, and establishes technical requirements and structure that include standard definitions of privacy policy components.

The Global Tech Framework describes the process to break down written policies into very specific and discreet components that enable a more effective and efficient means to automate policy enforcement. The basic concepts are described below:

Policy --- logical set of statements that dictate the conditions and scenarios for disclosing or withholding information. Each policy may have one or more Rules.

Rule(s) --- simple statements that authorize access or describe the conditions for exchanges. Each Rule includes Metadata Categories

Metadata Categories --- groups of standard terms and definitions that related to context, content, and decisions for information exchange. The Metadata Categories are the foundation for creating Rules, and the Tech Framework identified seven standard Metadata Categories

- DATA CATEGORIES - Properties of the data, including data type categories, associations of the data with persons and organizations, data classifications, and data quality information.

- PURPOSE - The business purposes for which private data was originally collected, or shared.

- USER CATEGORIES - Properties (attributes) about requestors who potentially access private data. These properties can be used to classify requestors (e.g., role, rights) and/or used to make dissemination decisions regarding certain pieces of data.

- CONDITIONS - Expressions that evaluate the context of a request for data. (e.g., the Subject must be in detention, and the user category must be Law Enforcement).

- OBLIGATIONS - Additional steps that a requestor is obligated to take after they receive the information.

- ACTIONS - Type of access (e.g., create, read, update, delete) to the information by the requestor.

- OUTCOMES - Privacy-relevant outcomes to a request (e.g., disclose, redact, withhold, notify).

By establishing these standard metadata categories and definitions, information sharing stakeholders can breakdown policies into simple statements, or rules, comprised of metadata values. The Tech Framework provides a basic narrative template to implement this technique.

Perform OUTCOMES in response to request for USER CATEGORIES to perform ACTIONS on DATA CATEGORIES under CONDITIONS for business PURPOSE subject to agreement to one or more OBLIGATIONS.

Here are two examples, related to access and modifications to a Warrant database, to demonstrate how to apply them in an information exchange among diverse stakeholders. (The quotes indicate example metadata values for each category).

Access:

Perform OUTCOMES "Disclose" in response to request for USER CATEGORIES "Sworn Law Enforcement" and "Law Enforcement ORIs" to perform ACTIONS "Read Access" on DATA CATEGORIES "NCIC Wants/Warrants Database" under CONDITIONS "Any Condition" for business PURPOSE "Wants/Warrants Check" subject to agreement to one or more OBLIGATIONS "Adherence to NCIC Usage policy".

Update/Modify:

Perform OUTCOMES "Allow" in response to request for USER CATEGORIES "Law Enforcement ORIs" to perform ACTIONS "Update Access" on DATA CATEGORIES "NCIC Wants/Warrants Records" under CONDITIONS "Originating Agency ORI" for business PURPOSE "Wants/Warrants Update" subject to agreement to one or more OBLIGATIONS "Adherence to NCIC Usage policy".

The complete list of Metadata Categories and definitions, as defined by the Privacy Tech Framework, are listed below. Users will define the individual values for each needed category.

- *Data Type*: groups of data with different privacy requirements (criminal, contact, location, physical, etc.)

- *Data Classification*: the level of authorization required to view or handle information

- *Source Reliability*: Indicates the reliability of the source that provided the information (reliable, not reliable, etc.)

- *Content Validity*: Indicates the accuracy or truth of the information (valid, not valid, etc.)

- *Business Purpose*: General category of why the information was collected or shared (officer safety, subject identification, etc.)

- *Requester Role*: The function or responsibility of an individual at their place of employment (law enforcement, attorney, judge)

- *Requester Rights*: The privileges or clearance levels granted to an individual certifications, training, licenses (NCIC, III, etc)

- *Level of Government*: Federal, state, municipal, tribal, other.

- *Retention*: Description of the timeframe for keeping or destroying information for a particular purpose (no retention, indefinite)

- *Dissemination*: Rules regarding sharing or distribution of information (no limitation, no dissemination)

- *Audit*: Rules regarding the logging of shared information (required, not required, annual)

- *Notifications*: Rules related to informing individuals or parties of shared information (subject, investigator)

- *Outcomes*: Actions resulting from an information sharing decision (allow, disclose, deny, redact)

SEARCH staff developed a Policy Reference Model, that includes pre-defined Metadata values fom the Privacy Tech Framework to create unique Rules and Policies. The Privacy Policy Reference Model is available at the JIEM Community Site under Reference Models.

Services

As service-oriented architecture (SOA) becomes more widespread in the justice, public safety, homeland security, and overall public sector domains, it is important for the JIEM methodology and tool to be able to tie core JIEM concepts (exchanges in particular) to services. SEARCH and BJA, under the guidance of the JIEM practitioner steering committee, decided to add a simple services dimension to JIEM as part of the Global Justice Information Sharing Initiative's effort to promote SOA for information sharing.

The concept of a service in JIEM is intended to align with the way "service" is defined in the Global Justice Reference Architecture (and the OASIS Reference Model for SOA.) As such, a service in JIEM is the means by which an organization gains access to a business capability owned, controlled, and managed by a partner organization. A service provides the consumer organization with a desired real-world effect produced by that capability.

For example, in the justice domain, a court generally has a court case management capability. This ability produces real-world effects such as calendaring cases, managing documents, recording decisions and judgments of the court, maintaining contact information for the parties, and so on. A citation filing service would provide access to a some of the real-world effects of court case management.

A service in the Global JRA has an "action model" that defines what a consumer may "do" with the service. In an integrated justice, public safety, or homeland security environment--indeed, in any integrated business enterprise--these actions manifest as information exchanges. Therefore, a service in JIEM associates to one or more information exchanges (objects in the exchange dimension).