Implementing Privacy Policy in Justice Information Sharing: A Technical Framework

by the Global Security Working Group

Technical Privacy Task Team

October 31, 2007

United States
Department of Justice

BJA

This project was supported by Grant No. 2005-NC-BX-K164 awarded by the Bureau of Justice Assistance, in collaboration with the U.S. Department of Justice's Global Justice Information Sharing Initiative. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the U.S. Department of Justice.

Table of Contents

Acknowledgements

The U.S. Department of Justice's Global Justice Information Sharing Initiative (Global) serves as a Federal Advisory Committee to the U.S. Attorney General on critical justice information sharing initiatives. Global promotes standards-based electronic information exchange to provide justice and public safety communities with timely, accurate, complete, and accessible information in a secure and trusted environment. Global is administered by the U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance.

Global aids its member organizations and the people they serve through a series of important initiatives. These include the facilitation of Global working groups. The Global Security Working Group (GSWG[1]) is one of four Global working groups covering critical topics such as intelligence, privacy, security, and standards. The GSWG is under the direction of Ms. Chelle Uecker, National Association for Court Management.

The *Implementing Privacy Policy in Justice Information Sharing: A Technical Framework* report was developed under the leadership of Mr. John Ruegg, Los Angeles County Information Systems Advisory Body. Global would also like to recognize the technical leads of the Technical Privacy Task Team for volunteering their time to the development of the *Implementing Privacy Policy in Justice Information Sharing: A Technical Framework*.

- Mr. John Ruegg—Los Angeles County Information Systems Advisory Body, Chair, GSWG Technical Privacy Task Team
- Mr. Joseph Alhadeff—Oracle, GSWG Technical Privacy Task Team
- Mr. Jim Cabral—IJIS Institute, GSWG Technical Privacy Task Team
- Alan Carlson, Esquire—The Justice Management Institute, GSWG Technical Privacy Task Team
- Mr. Scott Fairholm—National Center for State Courts, GSWG Technical Privacy Task Team
- Mr. Owen M. Greenspan—SEARCH, GSWG Technical Privacy Task Team
- Alan Harbitter, Ph.D.—IJIS Institute, GSWG Technical Privacy Task Team
- Erin Kenneally, Esquire—eLCHEMY, Inc., GSWG Technical Privacy Task Team
- Mr. Joe Mierwa—IJIS Institute, GSWG Technical Privacy Task Team
- Ms. Chelle Uecker—Superior Court of California, Chair, GSWG
- Mr. John Wandelt—Georgia Tech Research Institute, GSWG Technical Privacy Task Team

[1] For more information about the GSWG efforts, please refer to the Global Web site, http://it.ojp.gov/GSWG, for official announcements.

Intended Audience

Project Managers, Architects, and Technologists

This document is intended to provide guidelines for supporting the electronic expression of privacy policy and how to convert privacy policy so that it is understandable to computers and software. This report is intended as a resource for a technical audience, including Global Justice XML Data Model (GJXDM), National Information Exchange Model (NIEM), and Global Justice Reference Architecture (JRA) implementers, architects, developers, and system integrators, as well as other justice and public safety technical practitioners.

Executive Summary

As information sharing in the justice domain expands, it has become increasingly important to find ways to use technology to help implement and enforce protections of privacy, civil liberties, and civil rights. Converting privacy policy to a form understandable to computers continues to be a significant problem and a high priority for the justice community. *Implementing Privacy Policy in Justice Information Sharing: A Technical Framework* seeks to fill this need by exploring approaches and alternatives to resolve technical and interoperability challenges in supporting privacy policy through automation. The goal is to identify an approach and framework for protecting privacy which will be generally applicable to information sharing in the justice environment and which can be readily implemented using existing information technology architectures, standards, and software tools.

Implementing Privacy Policy in Justice Information Sharing: A Technical Framework builds on the previous work of Global and other federal and state groups. It begins with a review of basic privacy policy business requirements drawn from the Global Privacy and Information Quality Working Group's *Privacy Policy Development Guide and Implementation Templates*.

Based on these concepts, the privacy policy technical requirements were developed, including privacy policy metadata requirements. Once the business and technical requirements were documented, it was possible to define the privacy policy metadata and develop a standards-based approach for privacy policy implementation technical design. Parallel to this effort, a preliminary review was conducted of potential software alternatives available in the marketplace that could be used in the justice domain. These concepts were integrated into a Privacy Policy Technical Framework. This resulting approach is critical to supporting interoperability and is aligned with ongoing state, local, regional, and federal initiatives, such as NIEM and the Global Justice Reference Architecture.

Privacy Policy Technical Framework

The technical framework outlines a sequence of steps for implementing a set of electronic privacy policy rules. The electronic policy rules are designed based on written policies such as privacy policy documents, memoranda of understanding (MOU), and contracts. The framework requires all electronic information requests to be submitted with a set of electronic identity credentials to allow the policy service to determine whether the requestor has the authorization to access the information resource. The policy service is composed of software modules referred to as Policy Decision Points (PDP) and Policy Enforcement Points (PEP). The policy service ensures that the request is authenticated, authorized, and audited before granting access to the information resource. Additionally, the policy service may impose a set of obligations on the consumer regarding restrictions on further

information dissemination, record retention, and audit logging. A diagram depicting the high-level view of the technical framework appears below.

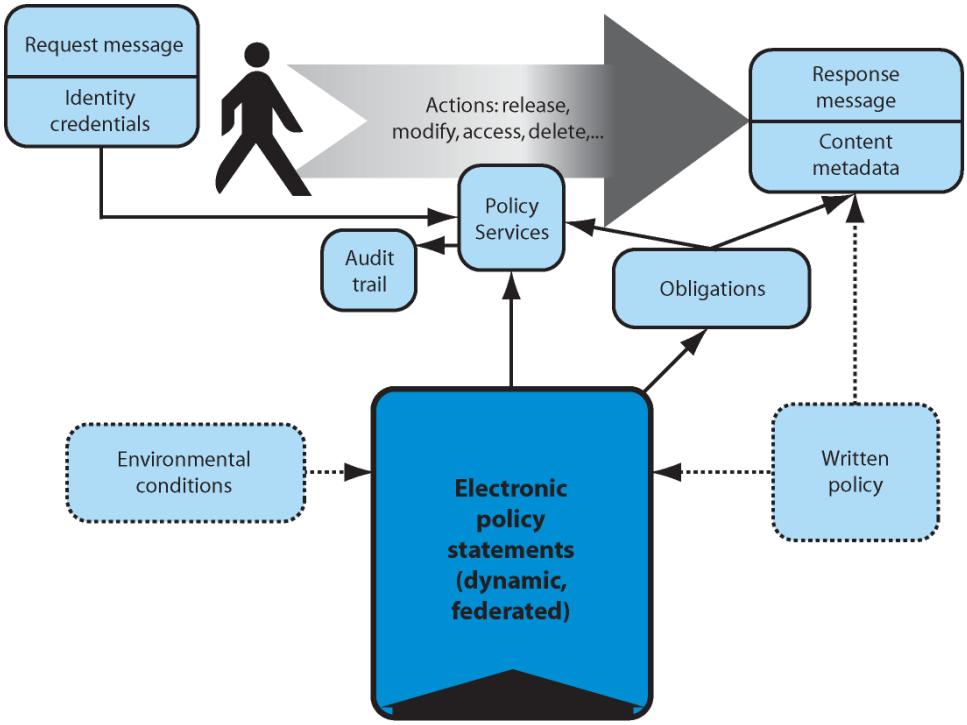


Figure 1: The Privacy Policy Technical Framework

Benefits of Policy Services

By adopting a common technical framework and justice domain vocabulary for expressing electronic policy rules, justice enterprises can better manage the security and access controls for their information resources, communicate their security and access control requirements to other justice agencies, and enable interoperable exchange of secure information by utilizing a common set of standards and policy metadata.

Historically, each information system programmed its own independent set of security and access controls, creating numerous silos of varied levels of information security policy enforcement throughout the enterprise.

The development of policy services as an independent set of security and access control services provides an enterprise with greater manageability for consistent implementation of policy across all of its information resources. Development of enterprise policy services affords opportunities for consistent reuse and standardization of policy administration. Separate policy services can be maintained without making expensive coding changes to the information systems governed by the policy services.

In today's environment of legal and regulatory requirements for information systems to be compliant with a myriad of policy requirements—such as the U.S. Privacy Act of 1974, Sarbanes-Oxley Act of 2002, the Health Insurance Portability and Accountability Act, and the Family Educational Rights and Privacy Act, to name a few—the design and implementation phase of enterprise policy services has become a strategic direction for reducing the risks of unauthorized disclosure of computer records.

1. Introduction and Purpose

1.1. Background

Many justice organizations have a critical business need to automate their real-world privacy policy and may be in the early stages of developing various approaches and alternatives to support automation of policy. To address this need, the Technical Privacy Task Team has compiled a set of technical requirements, specifications, industry standards, guidelines, and recommendations for applying technology mechanisms to support the electronic expression and enforcement of privacy policy. This resulting technical framework, called the Privacy Policy Technical Framework, can be used for illustrative purposes in discussing the approach developed by the Technical Privacy Task Team. This approach is aligned with the Global JRA, which provides the justice community with a reference body of work for the implementation of service-oriented architecture (SOA). *Implementing Privacy Policy in Justice Information Sharing: A Technical Framework* provides potential standards and specifications that will serve as guidelines and facilitate information sharing while ensuring a balance between effective information sharing and the implementation of privacy policy.

Implementing Privacy Policy in Justice Information Sharing: A Technical Framework builds on and therefore serves as a companion document to the following references:

- *Privacy Policy Development Guide and Implementation Templates*
- *Global Justice Reference Architecture Specification*, Version 1.4
- *Applying Security Practices to Justice Information Sharing*
- *Fusion Center Guidelines, Developing and Sharing Information and Intelligence in a New Era; Guidelines for Establishing and Operating Fusion Centers at the Local, State, and Federal Levels; Law Enforcement Intelligence, Public Safety, and the Private Sector*
- *Information Sharing Environment Implementation Plan*

1.2. Assumptions

The following assumptions were made by the Technical Privacy Task Team in developing this report:

1. This work product is intended to inform and support other groups and standards, such as NIEM and Global initiatives.
2. An agency has a preexisting privacy policy or will develop such a policy using other available work products and resources such as those referenced above.

3. A human-readable memorandum of understanding (MOU) regarding information sharing between agencies and Acceptable Use Policies will be required components for any privacy policy implementation.
4. Potential metadata categories required to support privacy policy will be forwarded to NIEM for vetting and incorporation into the data dictionary.
5. Sample use cases will be described for illustrative purposes only to demonstrate the use of the privacy framework and metadata categories.
6. This report is not exhaustive regarding the development of privacy metadata. Additional privacy metadata development will require detailed case study analysis and pilot privacy policy implementations.

1.3. Scope

Our focus is on the data about the people and organizations stored within information systems. This type of information is sometimes referred to as personally identifiable information (PII). This report will describe the electronic implementation of privacy policy by describing:

- Metadata associated with privacy
  - Specific to the justice domain
  - Relating both to the content of the data and the context in which it was collected or requested
- Technical framework
  - Technical mechanisms to define, enforce, monitor, and manage information exchanges subject to privacy policy requirements
  - Supporting a service-oriented architecture and identification of open standards for developing policy services
- Implementation guidelines
  - For further developing privacy metadata and electronic policy rules
  - For transitioning to enterprise electronic policy services

1.4. Out of Scope

The development of an organization's privacy policy was outside of the scope of the Technical Privacy Task Team. Instead of the development of policy, this report discusses the electronic implementation of privacy policy. The following security areas are also outside the scope of this report:

- Discussion of network, security administration, and perimeter security (such as network security, virtual private networks, network intrusion devices, anti-spam filters, anti-virus filters, and firewalls)
- Discussion of physical security best practices, such as locks on doors and paper shredding
- Encryption of data on mobile platforms (such as laptops and PDAs) and data breach prevention measures
- Discussion of governance and management structures to support privacy policy administration

1.5. Privacy Policy Requirements Overview

Policy represents a written set of rules governing the acceptable actions in a particular policy domain. Traditionally, policy and procedural manuals have been the primary means for documenting policies. Procurement policy, personnel policy, records management policy, and many other policies are based on a set of organization rules and one or more local, state, tribal, federal, and/or international laws and regulations. Transfer of records from one organization to another was subject to human review and done via postal mail and often only at the written request of or approval by the subject who wanted the records. Because electronic records exchange was the exception versus the rule, privacy was protected in part by the difficulty in accessing information, so-called "practical obscurity."

In today's information age, electronic data and documents can be rapidly exchanged among multitudes of organizations, each with its own, often conflicting policies. The electronic sharing of **PERSONAL INFORMATION** between organizations and the risk of inappropriate disclosure of personal information has stimulated concern about enforcing privacy laws and regulations governing disclosure of such information, including stiff financial or even civil and criminal penalties for violations of privacy policies. **PERSONALLY IDENTIFIABLE INFORMATION** (PII) is broadly defined to be one or more pieces of information that, when considered together or when considered in the context of how the information is presented or gathered, are sufficient to specify a unique individual.

Other laws require or restrict disclosure of information kept by government agencies about people, organizations, and their activities. Many state constitutions explicitly protect the public right to access information held by the government, and some state constitutions also protect privacy. Federal and state laws, such as freedom of information acts (FOIA) and public records acts, specify when information in government records must be disclosed and under what conditions the information can be withheld. Other laws protect specific types of information—for example, medical or mental health information, education information, and information about children—or limit disclosure of information to specific groups, such as law enforcement.

The Technical Privacy Task Team based the business requirements for electronically implementing privacy policy primarily from the *Privacy Policy Development Guide and Implementation Templates* ("Templates"). The Global Privacy and Information Quality Working Group developed the Templates to assist justice organizations in drafting privacy policies.

Table 1 itemizes the major privacy policy topics addressed in the Templates. The Technical Privacy Task Team analyzed the contents of each Section Heading to develop the privacy policy technical requirements and framework, which will be discussed in the next section of this report.

Privacy Policy Templates	
Reference	**Section Heading**
B.1.00	Statement of Purpose
B.2.00	Compliance With Laws Regarding Privacy, Civil Rights, and Civil Liberties
B.3.00	Definitions
B.4.00	Seeking and Retaining Information
B.4.10	What Information May Be Sought or Retained
B.4.20	Methods of Seeking or Receiving Information
B.4.30	Classification of Information Regarding Validity and Reliability
B.4.40	Classification of Information Regarding Limitations on Access and Disclosure
B.5.00	Information Quality
B.6.00	Collation and Analysis of Information
B.6.10	Collation and Analysis
B.6.20	Merging of Information From Different Sources
B.7.00	Sharing and Disclosure of Information
B.7.10	Sharing Information Within the Agency and With Other Justice System Partners
B.7.20	Sharing Information With Those Responsible for Public Protection, Safety, or Public Health
B.7.30	Sharing Information for Specific Purposes
B.7.40	Disclosing Information to the Public
B.7.50	Disclosing Information to the Individual About Whom Information Has Been Gathered
B.8.00	Information Retention and Destruction
B.8.10	Review of Information Regarding Retention
B.8.20	Destruction of Information
B.9.00	Accountability and Enforcement
B.9.10	Information System Transparency
B.9.20	Accountability for Activities
B.9.30	Enforcement
B.10.00	Training

Table 1: Privacy Policy Template Sections

2. Privacy Policy Technical Requirements

This section begins with a set of technical requirements that maps onto the **PRIVACY POLICY TECHNICAL FRAMEWORK.** For traceability, this section shows how the technical requirements link back to existing privacy policy business requirements. To validate the requirements, analysis of two different sample privacy policies is provided illustrating how the technical framework would be applied to real-life use cases.

Following the technical framework discussion, further technical detail is provided regarding the requirements for electronic policy statements. Privacy and quality metadata categories are defined for the purpose of establishing a justice domain-specific vocabulary of terms to describe the necessary elements for authoring electronic policy statements.

2.1. Privacy Policy Technical Framework

We expect technology to be able to implement the requirements of a policy built following the guidance in each section of the *Privacy Policy Development Guide and Implementation Templates* document (see Table 1). In Table 2, we itemize our expectations of privacy technology tools by section. Appendix A contains a mapping of the Templates business requirements to specific technical requirements. Appendix A also includes a requirements numbering scheme that traces back to the original Templates.

Reference Number	Privacy Policy Template Reference	Expectation of Technology
B.1.00	Statement of Purpose	Express the Statement of Purpose in a structured specification language that allows checking marked data for consistency.
B.2.00	Compliance With Laws Regarding Privacy, Civil Rights, and Civil Liberties	Express applicable laws in a specification language that allows checking marked data against policy for collection, use, and release.
B.3.00	Definitions	Convert domain-specific vocabulary into XML tags/values.
B.4.00	Seeking and Retaining Information	Provide a means to ask for information relevant to metadata to create the tags that will be used later and to check to make sure this person is allowed to gather and keep this type of information or is prevented by laws, such as the Fourth Amendment or First Amendment.
B.5.00	Information Quality	Provide a means to ask for metadata relevant to quality metatags, which will be added to the information. Also, check XML tags on data and credentials of individuals/organizations, and compare them to applicable electronic expression of policy to verify and mark (with XML) quality characteristics.
B.6.00	Collation and Analysis of Information	Verify the credentials of the individual requesting the analysis; confirm that the purpose of the analysis is consistent with policy and that all prerequisites have been met (e.g., confirm that collations are performed accurately against the same individual). Label the information postanalysis. Provide an audit trail.
B.7.00	Sharing and Disclosure of Information	Verify the identity of the information requestor (agency, subject, or public), the category of information, and release consistent with applicable electronic policy.
B.8.00	Information Retention and Destruction	Track the schedule for return, retention, and destruction. Make sure the required permissions and notifications are issued. Provide an audit trail.
B.9.00	Accountability and Enforcement	Implement information protection mechanisms that are consistent with monitoring compliance; for example, training requirements, audits, applicable technical standards, or benchmarks. Implement restrictions specified in enforcement policy (e.g., identify suspended or demoted individual and block access as appropriate).
B.10.00	Training	Train in use of technology implemented to support privacy policy.

Table 2: The Expectations of Technology in Supporting Requirements

Figure 2 presents a technical framework for technology used in implementing privacy policy, called the Privacy Policy Technical Framework. In describing this framework, we also reference metadata terminology defined by IBM's Enterprise Privacy Authorization Language (EPAL).[2] The EPAL terminology will be used in Section 2.3 of this document to organize metadata that may be of use for privacy policy enforcement in the justice community.

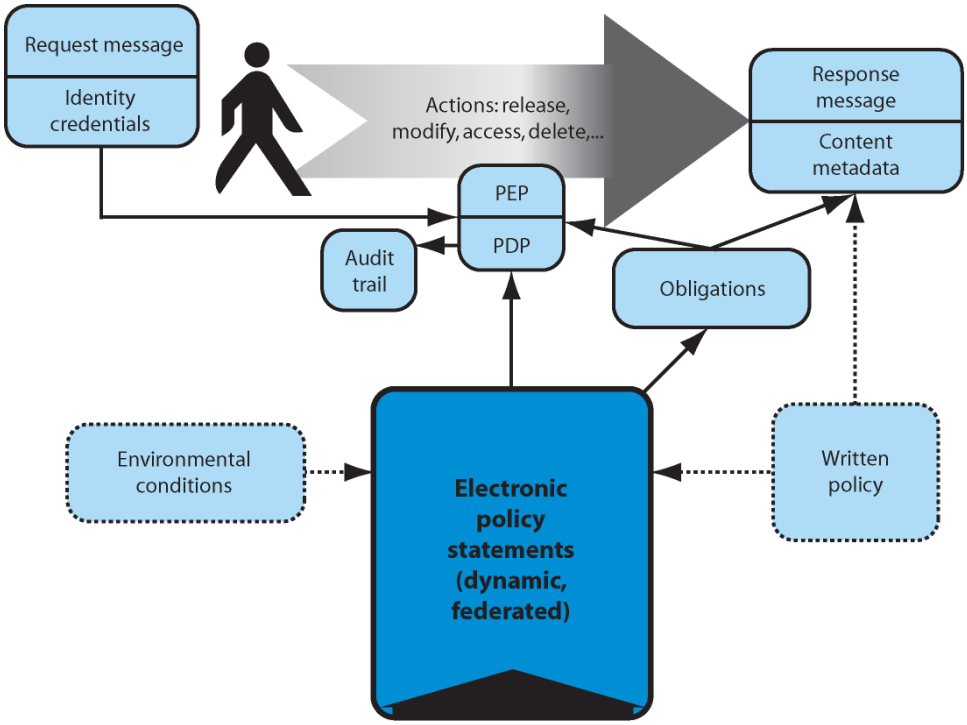


Figure 2: The Privacy Policy Technical Framework for Privacy Technical Requirements

There are six major Privacy Policy Technical Framework components identified shown above in Figure 2:

- Identity Credentials: Individuals (or organizations), internal or external to the justice community, will have identity credentials that can be applied in determining their rights to access or perform operations on information covered by a privacy policy. The EPAL term for this metadata is the *user category*. There is currently a Global Security Working Group initiative to develop guidelines for expressing user identity credentials in XML. This initiative is called Global Federated Identity and Privilege Management (GFIPM). We anticipate that GFIPM will eventually accommodate privacy requirements identified in conjunction with this Technical Privacy Task Team analysis.

[2] http://www.zurich.ibm.com/security/enterprise-privacy/epal/.

- Electronic Policy Statement: Portions of a privacy policy written in human-readable form should be convertible into an electronic policy statement—one that is interpretable by computer software. This statement will be encoded in a standardized Policy Assertion Language (PAL) such as eXtensible Access Control Markup Language (XACML). In EPAL, the policy is expressed as a combination of multiple metadata types (i.e., *user categories* are allowed or denied access to *content* under a given *context*). Figure 1 indicates that the electronic policy statement may be "federated" and may depend on external environment conditions. By "federated," we mean that the policy might include rules that are owned and managed by organizations external to those implementing them. By "depend on external environment conditions," we mean that the rules may be dynamic and change as a result of events or situational conditions in the external environment (e.g., changes in applicable laws or the national threat level changes to "severe").
- Content Metadata: There will be metadata associated with the information that is protected by the privacy policy. This metadata will characterize the information from a privacy perspective and link it to applicable rules in the electronic policy statement. In EPAL terminology, content metadata includes *data category* metadata and business *purpose* metadata.
- Policy Decision Point (PDP) and Policy Enforcement Point (PEP): The Policy Decision Point and Policy Enforcement Points sit between the user and information and allow or disallow operations requested to be performed on the information. The operations (e.g., release, modify, access, and delete) are drawn from the information flow illustrated above in Figure 1. These operations would be expressed as *action* metadata in EPAL terminology.
- Obligations: *Obligations* are requirements that a new caretaker of information agrees to when they take possession of information. Some of these obligations may be expressed as policy that is triggered when the information is accessed. Other obligations can be triggered by a timer. For example, obligations may include requirements such as "destroy this information after 60 days" or "remove all privacy restrictions after a year." Obligations can be used as a way of exporting policy from one organization to another.
- Audit Trail: Audit logs support the monitoring of policy compliance and provide the necessary elements to determine which organization or persons have accessed the information resource. The audit log can subsequently be used as a resource for identifying who needs to be notified when a previously disclosed record status has changed. Examples of record status changes include orders to seal or unseal records or changes in the data handling instructions or classification of the information.

Appendix A provides a detailed mapping of the Templates business requirements to technical requirements. Appendix B further refines the detailed technical requirements by mapping them to the components of the technical framework depicted in Figure 2. In some cases, the wording of the technical requirement has been modified slightly to make it applicable to the component. And in cases where a requirement is implemented differently

depending upon what component it is mapped to, a letter is added to the end of the requirements numbering scheme.

The mapping in Appendix B coupled with input from the Global Federated Identity and Privilege Management (GFIPM) initiative will guide the development of privacy policy metadata as discussed in Section 2.3. In addition, this input will assist in evaluating standards and tools that may be used to build the electronic policy statements and PDP/PEP components.

2.2. Privacy Policy Technical Framework Validation

The following paragraphs present an analysis of a sample privacy policy and a use case. This provides an initial validation of the business and technical requirements identified in Appendices A and B and illustrates how the technical framework may be applied.

2.2.1. Sample Privacy Policy Analysis

We selected a sample policy section at random from readily available justice community policy documents. Our sample is drawn from the *California Criminal Record Security: Statutes and Regulations*, dated August 2003. Although this reference is titled as a security policy, it also includes a privacy policy statement as well. The selected sample is entitled "Access to Information." The policy addresses the release of "criminal offender record information" and, in particular, when the subject of that information is a "*peace* officer or applicant for a position as a peace officer." Each paragraph of the policy was excerpted, followed by identification of the role of the applicable technical framework components and related justice system technical assumptions for validating a model implementation of the policy. The sample policy analysis can be found in Appendix C of this document.

2.2.2. Traffic Stop Use Case

To demonstrate how the technical framework might be applied, Figure 3 demonstrates a use case involving a traffic stop. In this traffic stop, a public safety officer requests criminal history information concerning a motor vehicle operator. In collecting this information, the officer uses software to determine that it may be appropriate to look for information in a jurisdiction with which the officer is not normally associated. The jurisdiction that holds the information has implemented a Web service to provide the information to the officer or other authorized requesting parties. The Web service checks the privacy policy protecting that information before providing it to any requesting party from an outside jurisdiction.

The following steps describe the events portrayed in Figure 3:

Traffic Stop Use Case	
Step 1	Using a mobile data terminal (MDT) in his/her patrol car, a public safety officer from jurisdiction "A" requests information on a motor vehicle operator. The software executing on the MDT requests the information by first accessing the enterprise policy (PDP/PEP) services offered by jurisdiction "B." (Alternatively, jurisdiction "B" could design the access so that the MDT accesses the Web service directly. The Web service then calls the policy (PDP/PEP), noted as Step 1a, Step 1b in the diagram.)
Step 2	The PDP/PEP in jurisdiction "B" examines the applicable electronic policy. The electronic policy indicates that the requestor must be from a "public agency or bona fide research body immediately concerned with the prevention or control of crime." Note that this wording is taken from the California policy but that there is no association between this use case and any systems in California.
Step 3	The PDP/PEP checks the credentials of the requesting officer.
Step 4	The PDP/PEP confirms that the credentials of the officer allow him/her to access the requested information as specified in the policy and permits release.
Step 5	The information is forwarded to the officer.

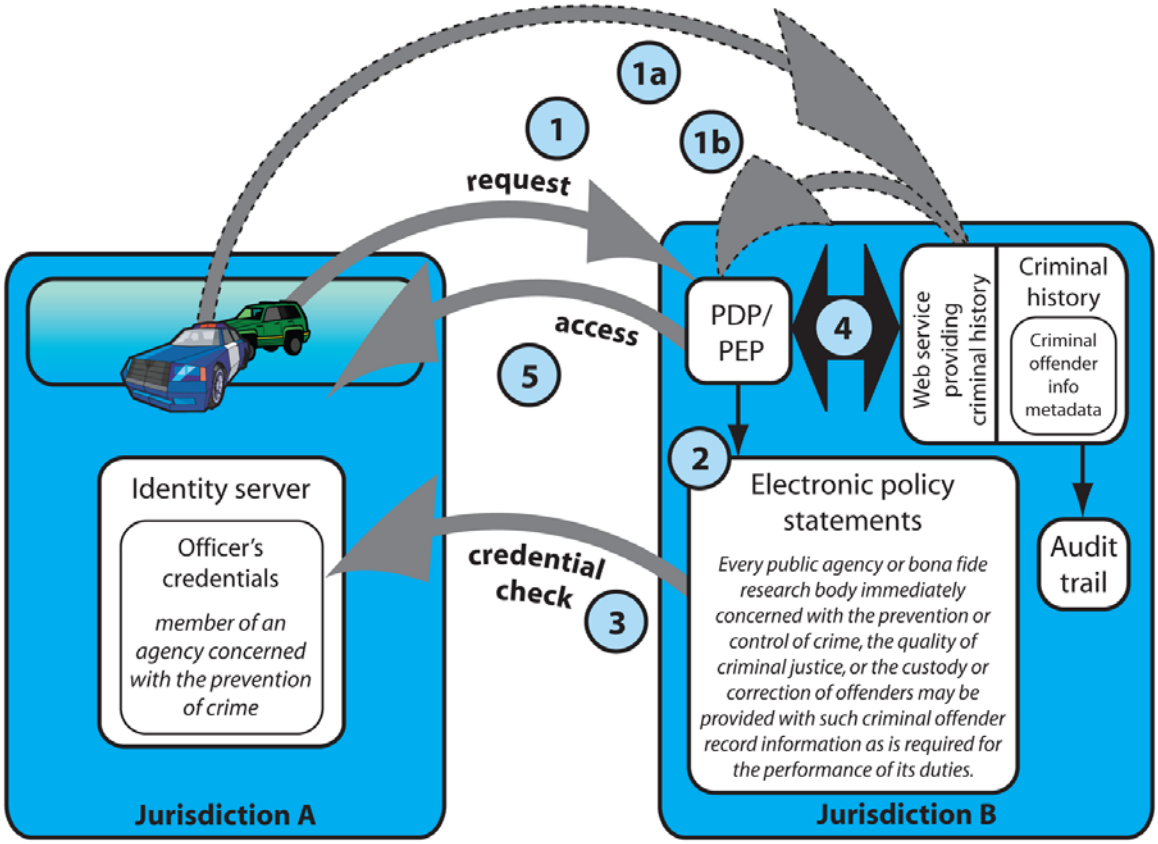


Figure 3: Case Study—A Traffic Stop

2.3. Privacy Policy Metadata Requirements

To support an interoperable understanding and exchange of electronic policy rules, a standard justice domain set of terms must be adopted. This section of the report outlines the categories of standard terms or metadata needed to author electronic policy rules for the justice domain.

These metadata requirements include the following: **CONTENT METADATA**, which describes the information being protected; **CONTEXT METADATA**, which describes the request and the current environment; and **DECISION METADATA**, which describes the outcome of the request:

- Content metadata
  - **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.
- Context metadata
  - **USER CATEGORIES**—Properties (attributes) about requestors who potentially access private data. These properties can be used to classify requestors (e.g., role) 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.
- Decision metadata
  - **OUTCOMES**—Privacy-relevant outcomes to a request (e.g., disclose, redact, withhold, notify).

Electronic policy statements utilize the metadata as variables in order to be evaluated for granting/denying access to privacy-related information. A generalized policy rule follows:

> Perform **OUTCOMES** in response to requests for **USER CATEGORIES** to perform **ACTIONS** on **DATA CATEGORIES** under **CONDITONS** for business **PURPOSE** subject to agreement to one or more **OBLIGATIONS**.

To develop an electronic privacy policy requires a justice domain-specific vocabulary of specific terms to describe the values for *user categories*, *data categories*, *business purposes*, and *obligations*. The resultant policy statements or rule set(s) would be designed to match the written privacy policy requirements. General *actions* metadata—such as add, copy, and modify—will often equate to specific service definition methods—such as addArrestRecord, getArrestRecord, or updateArrestRecord—and the range of valid values for *purposes* and *data categories* will also be specified during the service definition phase of developing a new service.

Although some metadata can be borrowed from industry standards, such as the Platform for Privacy Preferences (P3P), most metadata needed for privacy policy is fragmented and nonstandard among the justice agencies. This paper assumes that the GJXDM and NIEM represent the most developed domain-specific vocabulary for justice information systems. The metadata described in this paper leverages and could supplement the GJXDM and NIEM vocabularies.

The metadata defined in this paper leverages existing industry standards, privacy policy standards, GFIPM, and miscellaneous justice domain legacy metadata. Definitions of user-roles, affiliations, certifications, data classifications, data handling, and data reliability attributes are all examples of the types of metadata required to meet electronic privacy policy requirements.

Figure 4 depicts the initial metadata model for defining interoperable privacy policies.

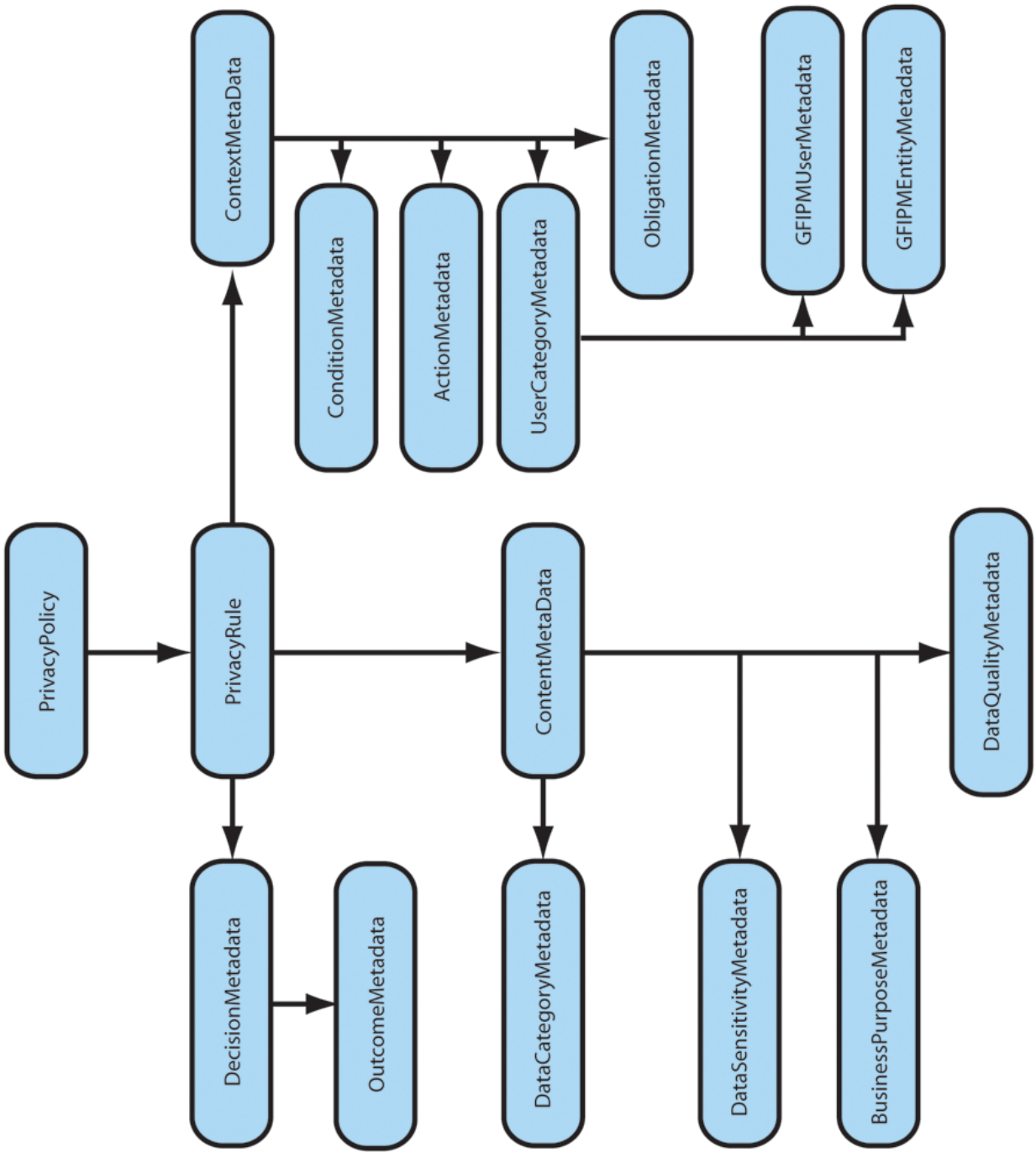


Figure 4: Privacy Policy Metadata Model

Detailed listings of the preliminary metadata list can be found in Appendix D: Privacy Policy Metadata Elements.

2.3.1. Level of Granularity for Privacy Policy

As in all policy design decisions regarding information security, the level of risk involved in erroneous release of information needs to guide the level of authentication and authorization rules that need to be developed in the electronic policy. An important design consideration in developing electronic privacy policy is determining the level of granularity the policy needs to address. In general, the more granular the policy becomes, the more costly it becomes to implement for both the information service provider and the service consumer. Some policies could be so complex that they require an interim manual step for a decision maker to evaluate whether the request will be granted or denied.

The same granularity rules apply to metadata. A policy written to permit law enforcement personnel access is at a much higher level of granularity and reuse than a policy written to grant access to a detective or investigating probation officer.

Applicable levels of granularity for privacy-related authorization services are defined as follows:

Coarse-Grained Authorization—Authenticated subjects within specific *user categories* are granted access to coarse-grained data objects. Familiar examples include role-based access to intelligence applications, Criminal Justice Information Services (CJIS) databases, unclassified documents, and incident reports. The user category gives access to all unclassified documents or database records within an application or service. These coarse-grained authorization rules have traditionally been embedded in application logic.

For example, the following authorization rule, is a coarse-grained authorization because access is to a coarse-grained data object, which, in this example, is all the records of the Wanted Persons Database:

> Perform **OUTCOMES** in response to requests for **USER CATEGORIES** "Law Enforcement ORIs" to perform **ACTIONS** "Read Access" on **DATA CATEGORIES** "NCIC Wanted Persons Database" under CONDITONS "Any Condition" for business **PURPOSE** "Wanted Persons Check" subject to agreement to one or more **OBLIGATIONS** "Adhere to NCIC Usage Policy."

Fine-Grained Authorization—Authenticated subjects within specific *user categories* are granted limited access to specific *data categories* of database records or specific application features based on both the *user category* and *data category* attributes, including a matching implied or explicit *business purpose*.

For example, the authorization rule:

> Perform **OUTCOMES** "Disclose" in response to requests for **USER CATEGORIES** "Law Enforcement ORIs" to perform **ACTIONS** "Modify Access" on **DATA CATEGORIES** "Criminal History Records" under **CONDITONS** "Records Created by the Source ORI" for business **PURPOSE** "Criminal History Record Updates" subject to agreement to one or more **OBLIGATIONS** "Adhere to NCIC Usage Policy."

is a fine-grained authorization rule because "Modify Access" is limited to specific records in the Criminal History System as opposed to any record in the Criminal History System.

Custom Authorization—Represents the policies that are so stringent or complex that they cannot be readily defined using a standard set of *user category* attributes and *data categories*. Because the authorization rules are customized for a specific set of resources, the policy is not reusable and there is no cost or benefit savings.

2.3.2. Enterprise Readiness for Fine-Grained Privacy Policy

Most legacy applications perform user registration, user authentication, role-based authorization, and fine-grained access control within the application logic. The trend towards building new services and applications with external user roles and attributes registered in directory services, such as Lightweight Directory Access Protocol (LDAP) and Active Directory, is enabling enterprises to start developing reusable, externalized security policies to control access to information resources. This trend will continue to evolve to the point where Identity Service Providers (IDP) will be able to manage the user identities and user roles for an organization and the IDPs will become the agent providing the necessary identity and access attributes required for accessing internal and external information resources.

Roles and attributes that define a role need to be commonly understood between the policy developer and the consumer of the service that needs to comply with the policy. It is unlikely that an enterprise would be able to support fine-grained authorization policy without first investing in and deploying coarse-grained authorization policies.

3. Industry Standards for the Privacy Policy Framework Components

As previously described in Section 2, the Privacy Policy Technical Framework for implementing privacy policy includes a set of technical components: Identity Credentials, Policy Decision Point (PDP)/Policy Enforcement Point(s) (PEP), Obligations, Content Metadata (Response Message), Electronic Policy Statements, and Audit module(s).

The following subsections address each of these components with regards to the open standards relevant to implementing the specific component.

3.1. Electronic Policy Statements

3.1.1. Electronic Policy Metadata Requirements

A machine-executable Policy Assertion Language (PAL) is needed to capture the electronic policy statements defined by the policy designer. The industry standards provide structures to define policy rules but do not provide the justice domain vocabulary metadata elements needed to author any specific policy rule. The initial set of required justice domain metadata is referenced in Appendix D. The major categories of metadata depicted in **bold** would be assembled using a PAL to specify a set of policy rules. Following is the general policy rule structure:

> Perform **OUTCOMES** in response to requests for **USER CATEGORIES** to perform **ACTIONS** on **DATA CATEGORIES** under **CONDITONS** for business **PURPOSE** subject to agreement to one or more **OBLIGATIONS**.

Obligations are a subset of the Service Provider Security and Privacy Policy Statements that are provided to the Service Consumer as policy for the consumer to implement. The Service Consumer is a secondary custodian of the information disclosed by the Service Provider. Service Consumer Obligations could include rules for purging personal data and auditing of all accesses both locally and back to the Service Provider and could even include links to written policy that consumers must acknowledge and agree to before obtaining access to the information.

3.1.2. Electronic Policy Assertion Languages (PAL)

There are a number of Policy Assertion Languages for defining electronic policies as described below:

Extensible Access Control Markup Language (XACML)—The majority of the technology vendor marketplace is investing in XACML-based tools for enterprise authorization, access

control, and electronic security and privacy policy development. XACML also has the advantage of leveraging the relatively mature XML standards for Web Services Security (WS-Security).

Extensible Rights Management Language (XrML)—The XrML standard is primarily applied in the consumer marketplace to protect digital media assets, such as movies, music, and video games. There are no interoperability standards for XrML.

WS-Policy—A set of standards to define and share policy documents. XACML is a Policy Assertion Language that provides a WS-Policy definition document and is considered to be contained within the WS-Policy standard.

WS-SecurityPolicy—A published WS-Policy PAL for specifying the set of security tokens, encryption, and message security requirements for a message to comply with in order to interact with an information service. This standard could be used, for example, to author a machine-readable Web service security policy based on the guidelines and requirements specified in the *Global Justice Reference Architecture (JRA) Web Services Service Interaction Profile* (WS SIP) document.

Platform for Privacy Preferences (P3P)—A consumer-selected set of privacy preferences utilized by a Web site to protect Web users' personal information. This standard has not been widely adopted.

New efforts for providing consumers with the ability to define their privacy preferences are under way with the Microsoft Cardspace program, ORACLE Identity Governance Framework, and the IBM Higgins Project. These efforts are early in their market maturity cycle and are more applicable to the consumer e-commerce market space versus the justice enterprise information sharing environment.

Although Policy Assertion Languages are maturing, the vendor marketplace is just beginning to develop policy-authoring tools that can be readily used by policy managers and business systems analysts. These policy-authoring products link a domain-specific vocabulary to the authoring tool and generate XACML as an output of the authoring tool. These tools should also provide an option to compile the XACML into a high-level programming code set such as .NET or java code for enhanced run-time performance.

3.1.3. Electronic Policy PDP/PEP Components

The Policy Decision Point (PDP) and Policy Enforcement Points (PEP) are the executable software/hardware modules that carry out the actions specified in the Electronic Policy Statements, such as grant/deny access, log message content, and permit limited access.

A variety of execution alternatives for implementing PDP/PEP components is offered in the vendor community, including platform vendor suites and single-focus vendor products.

These products integrate with existing database and/or Web application software and typically provide other policy development, deployment and management services. A representative set of vendor offerings is described in Section 5 and Appendix E.

3.2. Message Exchanges

In a service-oriented design approach, all communication between service requestor and service provider is achieved via electronic messages. The execution of the privacy policy could be designed as a set of common services, such as an authentication service, policy authorization service, and auditing service. These policy services would intercept the messages en route to the core information resource and perform the requisite security and privacy policy actions consistent with the policy requirements.

3.2.1 Identity Credentials and Message Content Metadata

Identity Credentials are the set of user categories and business purposes metadata that are inputs to the Electronic Policy Statements to evaluate whether to grant/deny access to the requested information resource(s). These products integrate with existing database and/or Web application software and typically provide other policy development, deployment, and management services. A representative set of vendor offerings is described in Appendix E.

3.2.2. Message Structure

The OASIS Web Services Security specifications (WSS 1.x) are a widely adopted set of interoperable XML standards for implementing message-level security for consumer and service provider authentication, message encryption, and transport of security assertions in SOAP-based messaging systems. The WSS 1.x may be specified for inclusion into reusable Service Interaction Profiles. The Service Interaction Profile could then be referenced by a number of enterprise services that share the same security and privacy policy requirements, leading to fewer overall policies and a more standard enterprise approach to service policy management. For a more thorough discussion of Service Interaction Profiles, the reader is referred to the *Global Justice Reference Architecture Specification* and the Web Services Service Interaction Profile.

3.3. Audit Services

The logging of authentication and authorization data is generally a policy requirement for any agency providing electronic access to justice information resources. The auditing and monitoring function requirements for privacy-related data access are no exception. The logged data must be of sufficient detail to identify unauthorized attempts to obtain secure information, to support detection of abnormal usage patterns, and to produce a variety of audit reports verifying conformance to the information service provider policies. The audit

logs become an information asset that must also be secured by the information service provider.

Following is a common privacy protection auditing/logging requirement for justice information sharing:

- An audit trail that minimally provides the ability to utilize the audit records for subsequent notification to electronic consumers of PII that the information has been corrected and/or sealed and needs to be updated in the consumers' system(s). Consumer systems, in turn, may be obligated to provide a similar notice for any secondary disclosures of the information.

Auditing tools exist in the marketplace to monitor compliance with security and privacy policy by detecting patterns of abuse and providing notifications for follow-up to administrators and policymakers of suspected abuse. A relatively new product space addressing Identity Management Auditing is included in Appendix E.

3.4. Standards for Sharing Security and Privacy Policies

Utilizing a standard justice domain-specific vocabulary (for example, NIEM or GJXDM) with the recommended standard will enable multiple justice agencies to discover and evaluate their capabilities to conform to the security and privacy policies of multiple jurisdictions. Standards for the electronic discovery and interchange of both human-readable and machine-readable policies are required to effectively communicate electronic policy, service-level agreements, MOUs, and written security and privacy policies. The following standards are relevant and consistent with the justice information sharing framework.

WS-PolicyAttachments—a component of the WS-Policy standard specifying how a policy is associated with an endpoint reference; Web service description; or Universal Description, Discovery, and Integration (UDDI) entry.

Security Assertion Markup Language (SAML)—specifically, the SAML 2.0 Profile for XACML, Version 2.0, provides a standard for transporting authentication tokens and XACML-compliant policy assertions in a federation and between a PDP and PEP.

Universal Description, Discovery, and Integration (UDDI)—an access protocol for publishing and retrieving policies from a registry.

WS-MetadataExchange—an interaction protocol for discovering and retrieving Web services metadata, including policy documents from a specific Internet address.

OASIS Web Services Secure Exchange (WS-SX)—has released a set of specifications to enable the establishment of trust among different domains utilizing a trust broker or security token service (STS) to support linking of two or more trust domains together, much like a gateway. The two specifications released to support these functions include WS-Trust and WS-SecureConversation. WS-Trust is utilized in some vendors' products to communicate between multiple PDPs/PEPs.

4. Privacy Policy Implementation Guidelines

Utilizing the set of policy definition standards, policy assertion languages, a domain-specific vocabulary of standard metadata, and mainstream message-level security profiles, the vendor community has provided a wide range of tools and execution environments for designing and implementing electronic security and privacy policy. Vendors' hardware and software components segregate or combine identity and access management, authorization policy execution, auditing and logging, and repository access in a multitude of ways.

4.1. Privacy Policy Business Requirements Analysis

Not unlike any other information system design methodology, the design of policy mechanisms for security and access controls follows the same steps of requirements definition, service design, configuration management, testing, implementation, and ongoing monitoring and maintenance of the policy service implementation. Unlike traditional application development, the security and policy services are developed externally, separate from the core application service functionality. The policy services become "middleware," executing between the service consumers and the information service providers.

Privacy policy design begins with evaluating current policy, laws, and regulations and determining whether the new information service requires the inclusion of **PERSONAL INFORMATION** or not. If it is determined that personal information is required for the information service to meet its business objectives, then a written policy should be drafted or referenced that details the privacy policy rules governing the new information service.

The privacy policy rules provide guidance on specifying the privacy policy metadata needed to author a set of machine-processable security and privacy policy rules, conditions, and actions. Based on the metadata types, metadata granularity required, and the security risks, a decision will be made as to which authorization model is most appropriate for the new information service (i.e., coarse-grained, fine-grained, or custom authorization).

The auditing and logging privacy policy requirements also need to be defined during the requirements analysis phase. The most common audit log consists of keeping a copy of the request message and reply message along with a log of the requestor authentication event and the policy action that was executed to grant or deny access. Alternatively, the designer may select specific elements describing the date and time of the request message, attributes on the requestor, status of the security verification (authentication event), policy evaluation outcome (grant or deny) or other disclosure status, and a copy of or reference to the information returned to the requestor. What is kept depends on the purpose of the logging and audits; that is, what does agency management want to be able to do with the audit information? Is it mostly preventative, or will active or random checking be done to check compliance?

4.2. Transition From Legacy Applications to Enterprise Policy Services

The electronic policy development and deployment strategy will vary depending on the organizational structure, political boundaries, and culture of the enterprise. The following sections outline design guidelines that could be applied for either a centralized set of policy services, a set of highly distributed policy services, or a hybrid approach.

Government agencies are not typically early adopters, and most justice agencies have shared databases secured only by private networks or online applications secured by username and password. The development of a service-oriented architecture and Web services has only been deployed in a minority of criminal justice agencies.

The transition from existing applications that contain authentication, authorization, and logging logic within the application to decoupled shared authentication, authorization, and logging services will evolve over time. The typical transition stages include:

- Stage 1—migrating to a shared Directory Service, such as LDAP or Active Directory, to maintain user attributes, perform local authentication, and support single sign-on capabilities. This stage externalizes the authentication event and provides a shared directory resource for user/application authorization attributes that can be utilized by multiple enterprise information services.
- Stage 2—develop a set of shared policy services external to the core application service logic. This stage moves coarse-grained and fine-grained authorization program logic code out of the core information service and into the shared policy services. These new executable modules are referred to as the Policy Decision Point (PDP) and Policy Enforcement Point (PEP) modules.

Most organizations are starting from an environment of applications with embedded authentication, authorization, and auditing program code as depicted below in Figure 5:

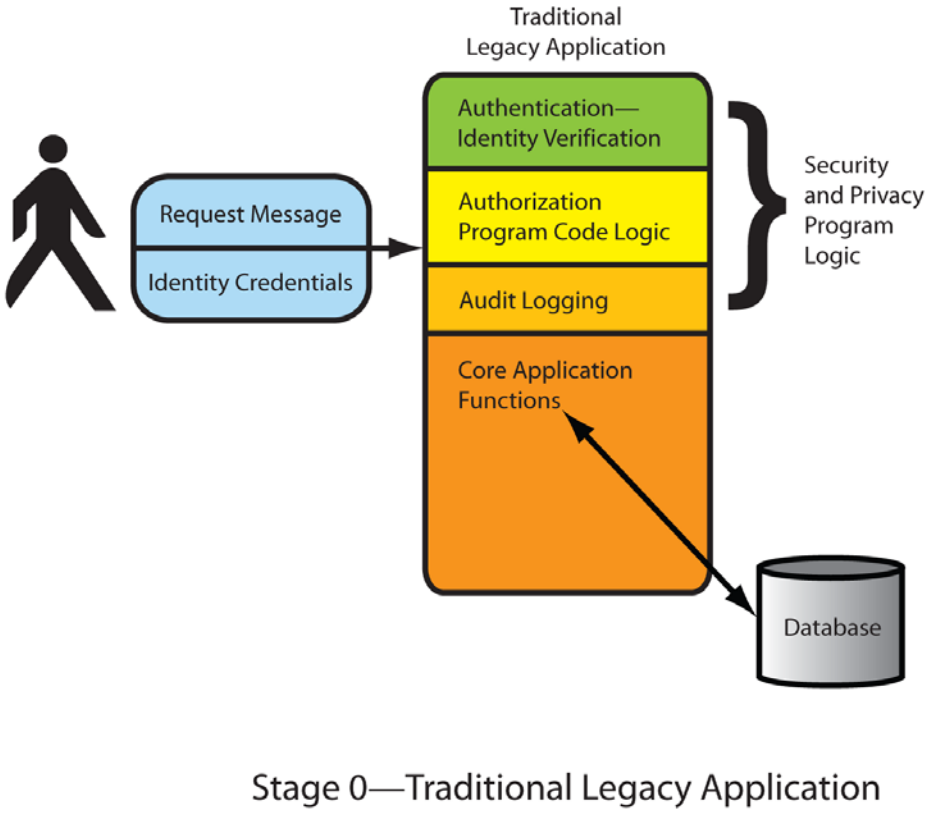


Figure 5: Privacy Policy Design—A Typical Justice Organization Representing Stage 0

The typical transition phases for justice organizations are depicted in Figures 6 and 7 below:

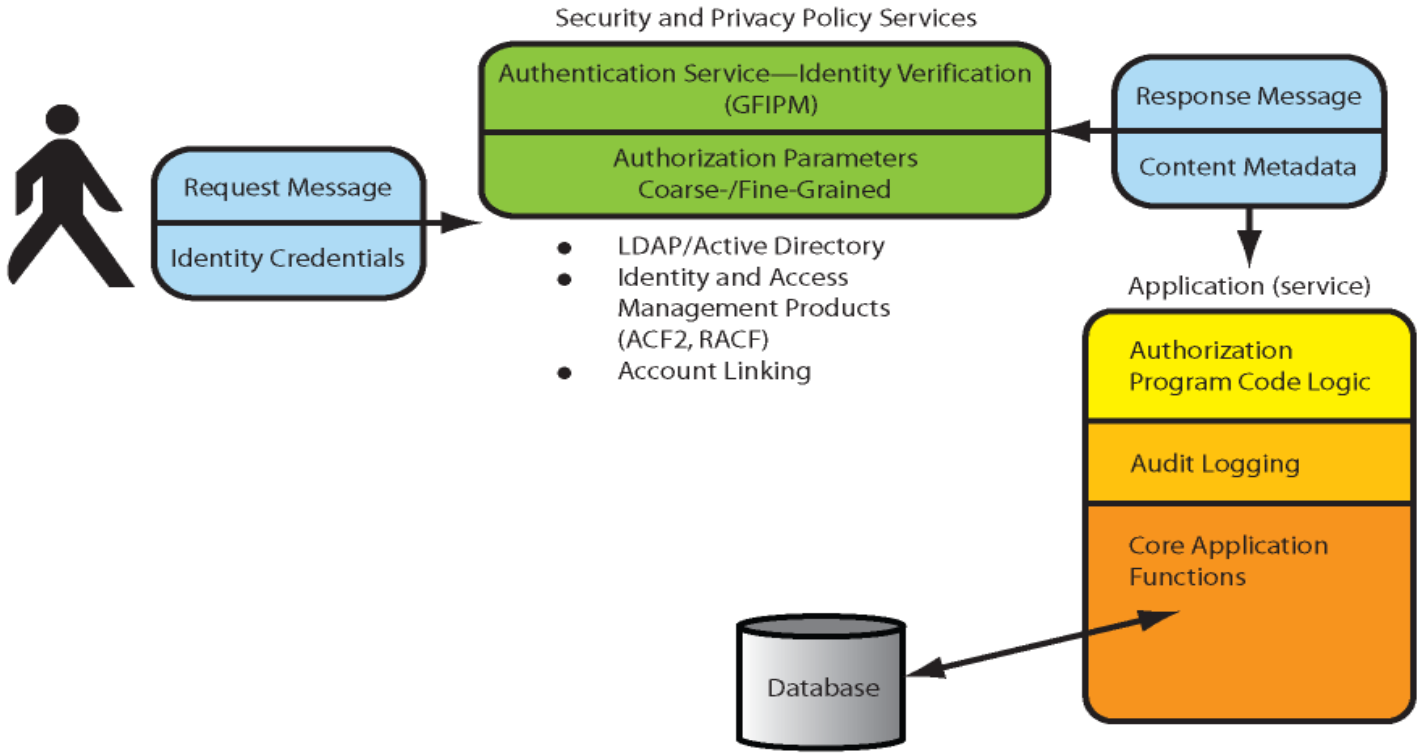


Figure 6: Privacy Policy Design—Potential Transition Step Representing Stage 1

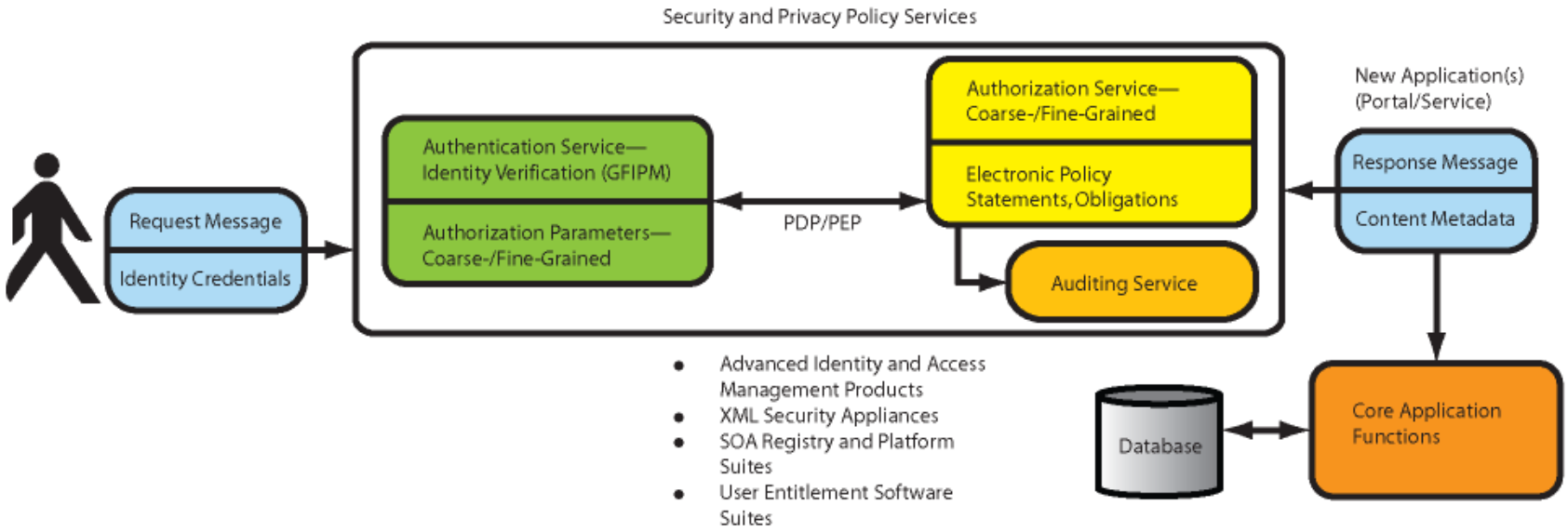


Figure 7: Privacy Policy Design—Final Transition Step Representing Stage 2

Stage 0 → Stage 1 Guidelines:

The transition to External Authentication Service(s) and Directory Services guidelines:

- Leverage legacy applications, existing authentication, authorization, and logging code versus rewriting that functionality when Web service enabling existing legacy applications.
- Design your policy authentication service to support both direct authentication and federated identity authentication services. The trend towards Identity Service Providers (IDP) is growing in the industry and is supported by the GFIPM.
- Federation enables more protection of PII by limiting the sharing of PII using, instead, pseudonyms or anonymous identifiers where appropriate instead of actual PII in the exchange. This is especially relevant for informants and victim/witnesses who have not consented to sharing their PII.

Stage 1 → Stage 2 Guidelines:

The transition to External Authorization and Auditing Service(s) guidelines:

- Develop external policy services for new SOA Services and portal and Web applications. Utilize legacy adapters to leverage systems with embedded authorization logic.
- To support fine-grained authorization control, acquire a commercial user entitlement management product, user-provisioning product, and/or role-based access management tool. Many of these products include audit logging and monitoring capabilities.
- Design the access control and privacy rules with the same standard, such as XACML. Privacy policy and access control are too tightly linked to each other to be treated as separate disciplines.
- Design the access control and privacy rules with an authoring tool that is usable by a policy analyst or system analyst versus coding in the native PAL, such as XACML. These tools are only now beginning to come to market.

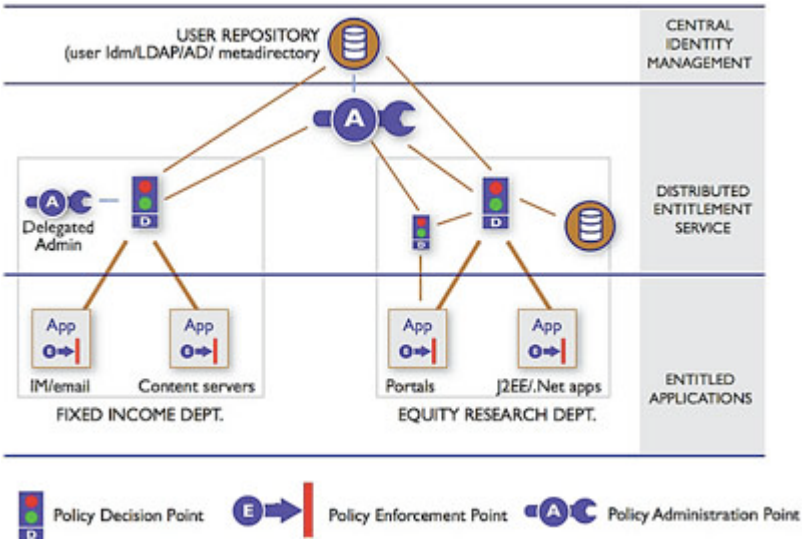
General Design Guidelines:

- Apply the right amount of electronic policy controls to balance the business requirements, protection, performance, and ease of administration. In general, the more fine-grained the policy controls, the higher the cost and complexity.
- Develop a procedure for correcting erroneous PII and for notifying subjects in the event of a data-breach to their PII.

- Ensure all hardware/software supports open standards such as those policy standards referenced in this report.
- Map legacy application-specific roles and new Services roles to NIEM and GJXDM roles for message exchanges.
- Build and support the Global Web Services Service Interaction Profile Username token profile, X.509 profile, and SAML profile for submitting Identity Credentials to the Policy Enforcement Point (PEP).
- Utilize NIEM and GJXDM for all message data and metadata attributes.
- Design the service policy for the minimum level of authorization granularity needed to meet the policy requirements. The coarse-grained authorization level is significantly cheaper to implement and maintain than fine-grained authorization, and custom authorization represents no cost-saving benefit due to lack of reusability.
- Design the information service to return content metadata for disclosed records. For example, include originating source, record-last-update, accuracy indicator, and special handling codes such that the consumer can evaluate the quality and sensitivity of the information returned.
- Design policy around consistent subsets of regulatory practice or model MOUs.
- Be practical; let MOUs and Policy Impact Assessments accomplish what is too complex or too custom to do in XACML.
- Provide an electronic link to the machine-readable, as well as the human-readable, set of policies and obligations a consumer must comply with as a condition of receiving PII.
- Define electronic policy using a common domain vocabulary of metadata terms. Section 2.3 of this report addresses privacy policy metadata categories with representative values described in Appendix D. Avoid the temptation to invent new data categories, roles, and business purposes. Instead, map internal roles to the common domain vocabulary roles for the purpose of data exchange and policy rule sets.
- Consider requiring auditing and logging as an obligation on the consumer system. For example, include requiring that an audit record be transmitted back to the original service provider each time the disseminated record is accessed within the consumer local system.

4.3. Privacy Policy Development Tools

The common terminology used to describe deployment of policy services includes the Policy Administration Point (PAP), Policy Decision Point (PDP), and Policy Enforcement Point (PEP). Some vendor products have combined these functions into one executable module; others have segregated each function into one or more intercommunicating modules. Following is a typical description of a vendor's offering set of features for electronic policy implementation.



Policy Administration Point (PAP)

The PAP provides centralized administration, management, and monitoring of entitlement policies, with delegation and integration with enterprise information repositories such as Active Directory and LDAP. The features of the PAP include:

- Browser-based, drag-and-drop user interface for creation of granular entitlement policies (based on user, resource, request context, action, and other environmental attributes)
- Sets per application as well as enterprise-wide policies
- Administer entitlements, including ability to group users and resources, clone and inherit entitlements, and delegate administration
- Manage, review, and audit all entitlement policies for all applications through a single centralized interface

Policy Decision Point (PDP)

The PDP provides run-time resolution of role-based and rule-based authorization policies. The PDPs are typically distributed in a high-availability configuration and can run on the same server as the application they are protecting.

- High-performance resolution of role-based and rule-based policies and management of distributed decision caches
- Snap-on integration with user information repositories (LDAP, Active Directory) and existing identity management solutions
- Flexibility in deploying the decision points to be local or remote to the resources for which they resolve the entitlement policies
- Standards-based solution with native support for XACML, SOAP, and SAML

Policy Enforcement Point (PEP)

PEPs enforce policy decisions made by the PDPs. The PEPs plug into standard J2EE and .NET application servers and also integrate with packaged applications such as portal, e-mail, messaging, content management, and Web servers.

Figure 8: Sample Vendor Offering for Implementing Policy Services

4.4. Mediation of Multiple Policies

The electronic resolution of multiple security policies is in a very early stage of development. The most recent progress in this area is with the WS-TRUST, WS-SecureConversation work, which supports the ability to broker security tokens between domains. For example, one enterprise may offer services based on a user ID and password basis, another using X.509 certificates, and the third using SAML authentication assertions. Utilizing an intermediary security token service (STS) and WS-TRUST, each of these entities could agree to trust the intermediary to convert the incoming security token to the desired security token of the receiving system, such as converting a username and password to an X.509 certificate or an X.509 certificate to a SAML authentication assertion.

Beyond this initial work in negotiating and brokering authentication tokens, there has been very little work in comparing authorization policies between domains. Until this area matures, designers of policy services will need to decide through negotiation and documentation of an MOU how to resolve conflicts in written policy between organizations. The decision to grant or deny an organization access to information will depend on whether the obligations of the service provider can be met by the consumer of the information.

The fusion center is a prime example of colocating, linking, or merging records from multiple agencies. Fusion centers must comply with multiple policy requirements and obligations for dissemination of records received from these outside agencies. The fusion center must ensure that each outside agency obligation is met as part of the fusion center dissemination of those records to fusion center subscribers. This will likely involve a significant degree of human-to-human negotiation and MOUs between the fusion center and information providers as well as the fusion center and information consumers.

In summary, the identity and access management, business purposes, obligations, auditing and logging, and policy rule sets should all strive to provide the minimum set of variables to achieve an acceptable level of risk for the information being protected.

5. Global Justice Reference Architecture (JRA) and Policy Services

As described in earlier sections of this report, implementation of privacy policy within an information system requires three basic functional services. Those technical services are an authentication service to validate identity, an authorization service to execute the privacy policy rules and actions, and an audit service to log incoming/outgoing messages for ongoing monitoring of the privacy policy implementation.

The industry trend is to provision authentication, authorization, and auditing as a set of intermediary shared services deployed externally to the core information resource delivery service. As noted in the vendor product review section of this report, multiple alternatives exist for provisioning these services, including dedicated XML Security appliances, registry vendor products, and components of platform vendor suites, as well as point-specific products focused on administration of role-based entitlements for service consumers.

To meet the major goal of enabling greater electronic information sharing among justice agencies while ensuring privacy, civil rights, and civil liberties dictates a number of technical subgoals to be met. These goals include standardization of vocabulary (for example, NIEM and GJXDM) and a common technical framework (such as Global JRA specifications, terminology, and concepts), along with standards that support interoperability, reliability, confidentiality, integrity, authentication, authorization, and auditability.

The Global Justice Reference Architecture identifies a set of conceptual components that are required to build a set of loosely coupled *Service(s)*. Figure 9 below depicts the current JRA conceptual model.

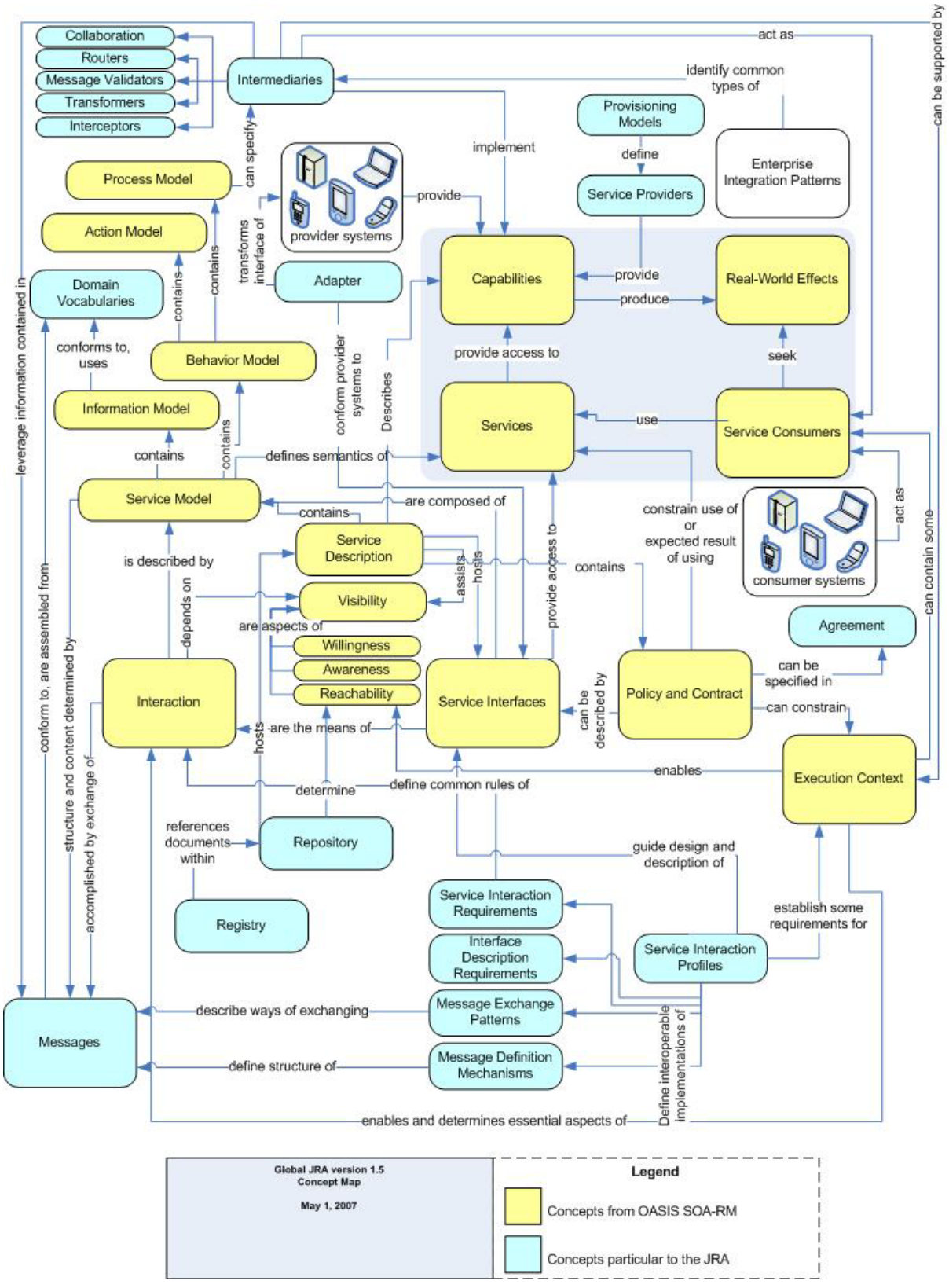


Figure 9: Global JRA Conceptual Model

Policies and Contracts—This JRA component is the primary domain for defining human-readable and machine-readable policy, privacy policy (authorization policy), audit policy, service-level agreements, and identity and authentication policy.

Visibility—The privacy policy requirements and obligations for a service must be known before a service consumer can interact with a service provider service. The policy service interaction requirements must be stored in some reachable persistent storage repository. This repository is sometimes referred to as a policy server or metadata server. The standards available for providing visibility include:

- WS-Policy
  - WS-PolicyAttachment
  - WS-SecurityPolicy
  - WS-PolicyAssertions
- UDDI, Registry Access
- Web Site Publication of Services
- WS-MetadataExchange

Domain Vocabulary—The set of privacy metadata and policy content elements required to support the privacy policy rules should be available in the domain vocabulary.

Behavior Model—For a privacy policy service, the behavior model would specify the privacy policy rules, including the authentication, auditing, and obligations specifications. The behavior model would be specified using a policy-authoring tool that generates a PAL such as XACML. WS-SecurityPolicy provides a PAL for defining authentication requirements. The specific policy metadata values for *user categories*, *actions*, *data categories*, *purposes*, and *obligations* would be described at the same time the behavior model for the core information service was being defined. The service policy rules would be authored using a PAL such as XACML.

Information Model—The metadata required to build a set of policy rules represents the information model for policy definition. The privacy metadata could become additional elements and attributes within the NIEM/GJXDM information model or a separate information model linked to NIEM/GJXDM.

Messages—All service interaction is performed via exchange of messages. Therefore, the messages must convey all service consumer authentication and authorization attributes necessary for the service provider policy service(s) to be executed. These intermediary policy services are depicted in the diagram below:

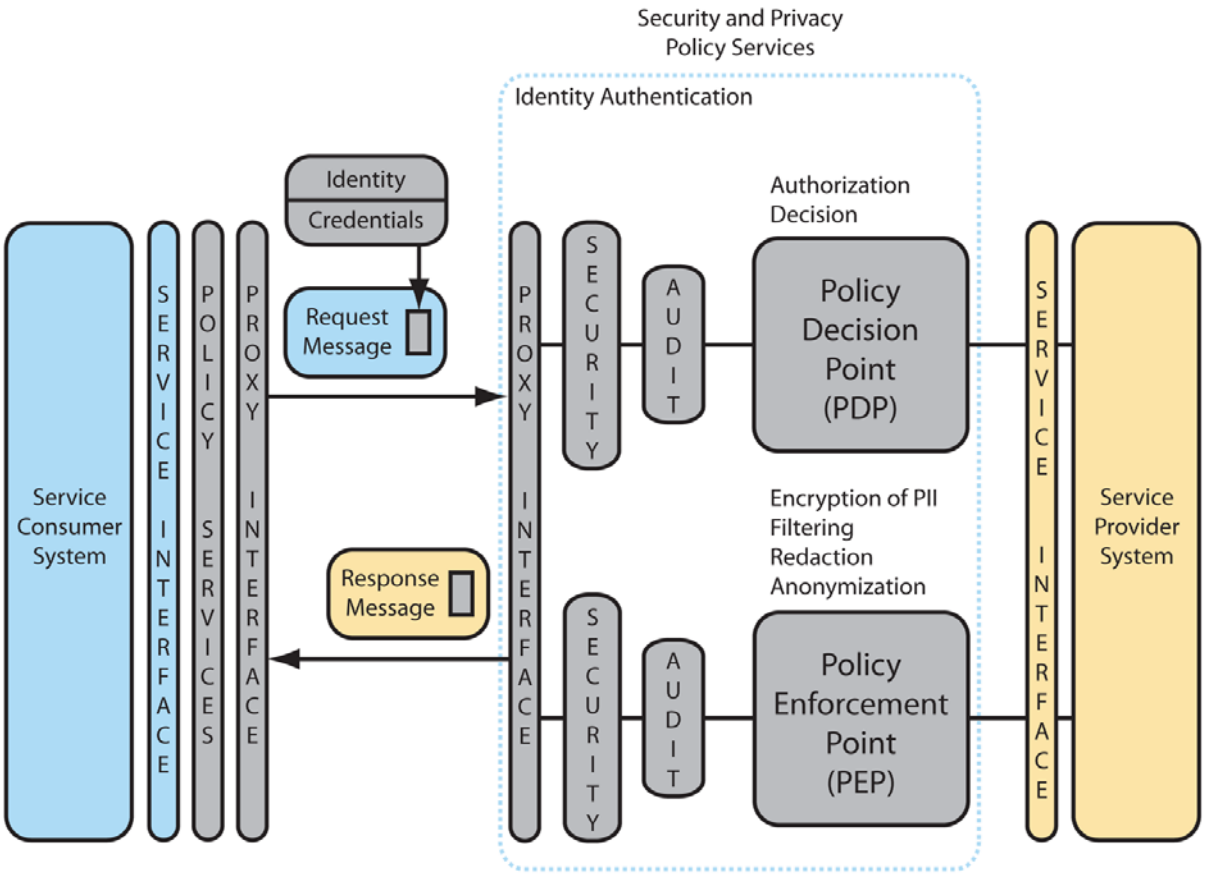


Figure 10: Global JRA Integration of Policy Attributes for Centralized Policy Enforcement Model

Figure 10 depicts the transport of policy attributes in the small colored box contained within the message. In this design, the policy interface is the intermediate service interface for the request message. The security service performs authentication or validates the federated authentication assertion and may perform other message validation functions. The audit service will log the required message information per the service provider policy requirements. The Policy Decision Point (PDP) and Policy Enforcement Point (PEP) are the services that evaluate the request message policy attributes and message elements to determine what content will be returned in the response message.

Figure 11 depicts an alternative design in which each service provider determines whether an intermediary policy service will be invoked to meet policy requirements. The selection of the more centralized policy enforcement model in Figure 10 or decentralized model in Figure 11 will be determined by the information technology governance model for the implementing organization.

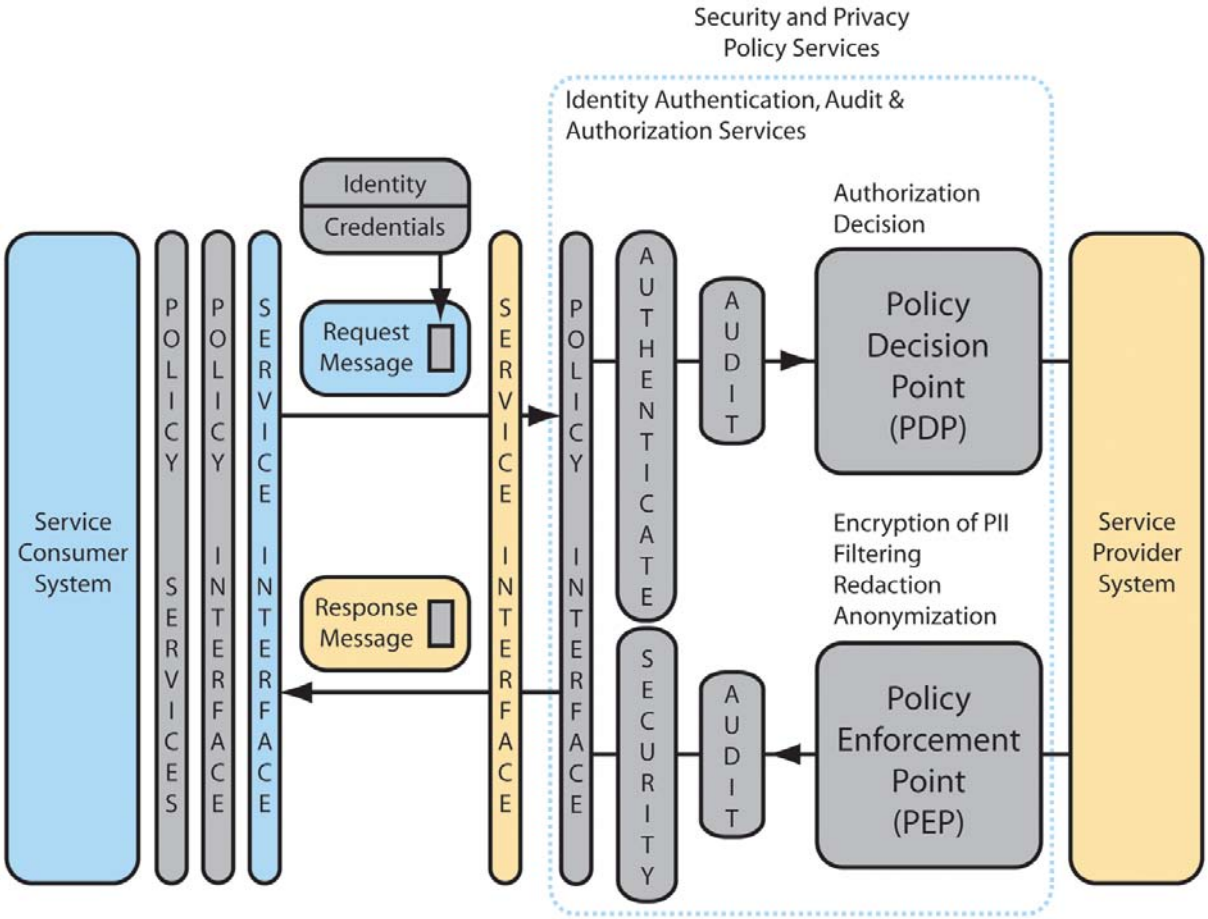


Figure 11: Global JRA Integration of Policy Attributes for Decentralized Policy Enforcement Model

Service Interaction Profiles—Provide interoperable message structures for including policy assertions (identity tokens, user-credentials authorization attributes, privacy preferences) in the service interaction message(s). The supported tokens, assertions, etc., would be defined in the PAL. (See behavior model description above.)

Execution Context—As noted in the vendor product review, a typical execution context provisions contracts and policies functionality as a set of services external to the information delivery service. (See Appendix E). The authentication service, authorization service, and auditing service become a set of "shared services" or "agents" utilized by the service provider to implement policy constraints on the information resources being made available as a service. Each core information resource service, in effect, specifies a set of external electronic policy statements that governs the content the service will accept and distribute.

6. Summary Recommendations

The following is a high-level list of recommendations for implementing security and privacy policy:

For Implementers:

- Adopt the proposed Privacy Policy Technical Framework for all new applications (such as Global JRA Services, portals, and Web applications).
- Adopt XACML as the executable and exchangeable PAL for defining electronic privacy policy. For interoperability purposes, it is recommended that the justice community select from commercial products that provide a nontechnical policy-authoring tool that can generate XACML and other run-time executables generated from XACML.

For Global:

- Recommend that NIEM, through the NIEM Technical Architecture Committee and the NIEM Business Architecture Committee, and Global leadership in the form of the Global XML Structure Task Force (GXSTF) adopt the privacy policy metadata model defined in this report. Additionally, evaluate and recommend whether the information model for the privacy policy metadata should be separate or included within the NIEM/GJXDM information model.

7. Next Steps

The following actionable items are recommended as the next steps for consideration by Global leadership as well as the justice community:

- Fund privacy policy pilot projects under direction of a Global task team to continue development of the Privacy Policy Technical Framework:
  - Pilot commercial product implementation of external Authentication, Authorization (PDP/PEP), and Auditing services supporting both coarse-grained and fine-grained privacy policy rules enforcement within the proposed Privacy Policy Technical Framework.
  - Develop a repository of Executable Policy Rule(s) templates based on the selected pilot(s) policy implementations.
  - Utilize GFIPM and NIEM for transmittal of privacy policy user categories and authorization attributes.
  - Utilize Global JRA Service Interaction Profiles (SIPs) to send Identity Credentials to commercial PEP/PDP products.
  - Vet and supplement/modify the initial list of privacy metadata consistent with the pilot project outcomes.
  - Further define strategies for leveraging the authentication, authorization, and auditing logic of legacy applications while developing the infrastructure to support the Privacy Policy Technical Framework for new applications.
  - Test/refine the methodology for translating real-world privacy policies to electronic policy statements, and evaluate the cost, performance, and lessons learned.
  - Evaluate feasibility of augmenting the SEARCH Justice Information Exchange Model (JIEM) tool to define policy constraints for common information exchanges.
- Continue work efforts to integrate the Privacy Policy Technical Framework into JRA environments.
  - Develop the policy services consistent with Global JRA Specifications, and validate the JRA components' relationship to the privacy policy services components.
- Encourage the justice community to continue to validate the privacy metadata within their own operating environments.
  - Support the development of the capability to use more "fine-grained" decisions through the use of privacy metadata, such as those proposed in this report.

Appendices

Appendix A: Detailed Technical Privacy Requirements

Technical Requirement Number	Technical Requirement Description
BT.1.0x	1. Express "Statement of Purpose," in whole or in part, in a machine-understandable format.
BT.2.0x	1. Translate the statement of the law into machine-understandable constraints on actions under the headings of collection, use, analysis, retention, destruction, sharing, and disclosure of information.
BT.3.0x	1. Express the appropriate terms as subjects, objects, or other elements of the policy in terms consistent with the electronic policy syntax and semantics.
BT.4.00	
BT.4.1x	1. There shall be mechanisms to identify incoming information and associate it with the purpose information statement in B.1.00. 2. There shall be mechanisms to label incoming information as it is stored and bind a purpose statement to it. 3. There shall be mechanisms to reject incoming information that does not comply with the purpose statement. 4. Provide naming conventions for Records Management System (RMS), Computer-Aided Dispatch (CAD), Case Management System (CMS), Jail Management System (JMS), Criminal Justice Information Services (CJIS), and/or Integrated Justice Information System (IJIS) systems. 5. Identify information as pertaining to the stage of the proceeding; for example, an ongoing investigation; enforcement activity; criminal history; religious, political, or social views; identifying an individual; or the need to provide services or accommodate religious, ethnic, or cultural obligations. 6. Provide a mechanism to delete information collected from unauthorized or prohibited sources. 7. Enforce information retention policy.
BT.4.2x	1. Identify and categorize the provider of information. 2. Accept collection from authorized providers and block collection from unauthorized or illegal providers.
BT.4.3x	1. Categorize and label retained information regarding its content validity, nature of the source, and source reliability. 2. Provide a vocabulary for describing content validity, nature of the source, and source reliability.
BT.4.4x	1. Categorize and label retained information regarding limitations on access and disclosure. 2. Provide a vocabulary for describing limitations on access and disclosure. 3. Define criteria and mechanisms for reevaluating classification. 4. Link classification to status of the subject individual (e.g., victims of domestic violence crimes may have unique release policies).
BT.5.0x	1. Provide labeling and verification mechanisms to ensure that information is (1) derived from dependable and trustworthy sources of information; (2) accurate; (3) current; (4) complete, including the relevant context in which it was sought or received and other related information; and (5) merged with other information about the same individual or organization only when the applicable standard (in Section B.6.20) has been met. If the information does not have

Technical Requirement Number	Technical Requirement Description
	some of these qualities and will still be kept, the quality concerns must be indicated in the quality metadata. 2. Provide a mechanism to schedule reevaluation of quality and reliability of information. 3. Provide a mechanism to detect or investigate and delete erroneous, misleading, obsolete, or unreliable information. 4. Provide a mechanism to delete information collected from unauthorized or prohibited sources.
BT.6.0x	
BT.6.1x	1. Provide a mechanism to confirm that collation and analysis is not being conducted for a reason other than that identified in "statement of purpose." 2. Provide a mechanism to authenticate and authorize the credentials of the individual requesting the collation and analysis. 3. Provide a mechanism to label the resultant information with appropriate privacy policy constraints and categorizations.
BT.6.2x	1. Provide mechanisms to express, in electronically readable format, prerequisites for merging. 2. Include confirmation that two sources of information address the same individual or organization. 3. Provide mechanisms to block merging if prerequisites are not met or to include metadata that the match may not be conclusive but seems probable.
BT.7.0x	
BT.7.1x	1. Define subject names for the appropriate user group and role associations to name in the policy. 2. Provide the ability to associate law enforcement, public protection, public prosecution, public health, and justice purpose with an access request. 3. Provide the ability to accept or deny a request to access information based on user group, role, and purpose. 4. Maintain an audit trail for access or dissemination.
BT.7.2x	1. Define subject names for the appropriate external user group and role associations to name in the policy. 2. Same as BT.7.1x, items 1–4, but add "avoid imminent danger or certain danger to life or property" as a purpose and allow exceptions based on this purpose.
BT.7.3x	1. Define "specific purposes" in a machine-readable form. 2. Mark information to associate with those specific purposes. 3. Positively identify individuals that have access to information under those purposes. 4. Enforce rules that release information under the specific purpose to be authenticated.
BT.7.4x	1. Mark information as accessible to the public. 2. Enforce rules that govern the release of information to the public.
BT.7.5x	1. Positively identify individuals outside the agency. 2. Accurately track information to subject and correlate with authenticated individual. 3. Enforce disclosure policy based on BT.7.4x, items 1–2.
BT.8.0x	1. Set up schedule for information review.

Technical Requirement Number	Technical Requirement Description
	2. Scan marked information and invoke actions (retain, destroy, or return). 3. As required, seek approval before action. 4. As required, notify appropriate parties of action. 5. Record actions.
BT.8.1x	See BT.8.0x above.
BT.8.2x	See BT.8.0x above.
BT.9.0x	
BT.9.1x	1. Provide a means to satisfy requests from the public to access the policy.
BT.9.2x	1. Implement information protection mechanisms that are consistent with applicable technical standards or benchmarks.
BT.9.3x	1. Implement restrictions specified in enforcement policy (e.g., identify suspended or demoted individual and block access as appropriate).
BT.10.0x	1. Provide training on using and administering privacy mechanisms.

Appendix B: Mapping of Technical Requirements Onto the Framework

Technical Requirement Category	Identity Credentials (1) (User Categories, Purpose Metadata)	Electronic Policy Rules (2) (Conditions, Obligations Metadata)	Content Metadata (Data Categories, Purpose Metadata)	PDP/PEP (3) (Actions, Obligations Metadata)
BT.1.0x Statement of Purpose		BT.1.01. Express "statement of purpose," in whole or in part, in a machine-understandable format.		
BT.2.0x Compliance With Laws Regarding Privacy, Civil Rights, and Civil Liberties		BT.2.01. Translate the statement of the law into machine-understandable constraints on actions under the headings of collection, use, analysis, retention, destruction, sharing, and disclosure of information. Provide a structure so that policy statements can be tracked to a legal hierarchy (e.g., state law supersedes local law; local law supersedes agency policy).		
BT.3.0x Definitions	BT3.01a. Express the appropriate terms for subjects, objects, or other elements of the policy in terms consistent with the electronic policy syntax and semantics.	BT3.01b. Express the appropriate terms for subjects, objects, or other elements of the policy in terms consistent with the electronic policy syntax and semantics.	BT3.01c. Express the appropriate terms for subjects, objects, or other elements of the policy in terms consistent with the electronic policy syntax and semantics.	
BT.4.0x Seeking and Retaining Information	BT.4.16a. Identify who may/must approve retention decisions.	BT.4.16b. Express the information retention policy.	BT.4.11a. There shall be labels to identify incoming information and associate it with the purpose information statement in B.1.00. BT.4.14. Provide naming conventions for RMS, CAD, CMS, JMS, CJIS, and/or IJIS systems. BT.4.15. Identify information	BT.4.11b. Provide mechanisms to identify incoming information and associate it with the purpose information statement in B.1.00. BT.4.12. Provide mechanisms to label incoming information as it is stored and bind a purpose statement to it. BT.4.13. Provide mechanisms to reject incoming information that

Technical Requirement Category	Identity Credentials (1) (User Categories, Purpose Metadata)	Electronic Policy Rules (2) (Conditions, Obligations Metadata)	Content Metadata (Data Categories, Purpose Metadata)	PDP/PEP (3) (Actions, Obligations Metadata)
			as pertaining to an ongoing investigation; enforcement activity; criminal history; religious, political, or social views; identifying an individual; or the need to provide services or accommodate religious, ethnic, or cultural obligations. BT.4.16a. Label data to support the enforcement of information retention policy.	does not comply with the purpose statement. BT.4.16b. Enforce information retention policy.
			BT.4.21. Identify and categorize the source of information.	BT.4.22. Block collection from unauthorized or illegal sources.
			BT.4.31. Categorize and label retained information regarding its content validity, nature of the source, and source reliability. BT.4.32. Provide a vocabulary for describing content validity, nature of the source, and source reliability.	
		BT.4.43. Define criteria and mechanisms for reevaluating classification. BT.4.44a. Link classification to status of the subject individual (e.g., victims of domestic violence crimes may have unique release policies).	BT.4.41. Provide a vocabulary for describing limitations on access and disclosure. BT.4.44b. Provide a vocabulary to classify the status of the subject individual (e.g., victims of	BT.4.42. Categorize and label retained information regarding limitations on access and disclosure.

Technical Requirement Category	Identity Credentials (1) (User Categories, Purpose Metadata)	Electronic Policy Rules (2) (Conditions, Obligations Metadata)	Content Metadata (Data Categories, Purpose Metadata)	PDP/PEP (3) (Actions, Obligations Metadata)
			domestic violence crimes may have unique release policies).	
BT.5.0x Information Quality			BT.5.01. Provide labeling and verification mechanisms to ensure that information is (1) derived from dependable and trustworthy sources of information; (2) accurate; (3) current; (4) complete, including the relevant context in which it was sought or received and other related information; and (5) merged with other information about the same individual or organization only when the applicable standard has been met.	BT.5.02. Provide a mechanism to schedule reevaluation. BT.5.03. Provide a mechanism to delete erroneous, misleading, obsolete, or unreliable information. BT.5.04. Provide a mechanism to delete information collected from unauthorized or prohibited sources.
BT.6.0x Collation and Analysis of Information	BT.6.12a. Provide credentials to the individual requesting the collation and analysis.			BT.6.11. Provide a mechanism to confirm that collation and analysis are not being conducted for a reason other than that identified in "statement of purpose." BT.6.12b. Provide a mechanism to authenticate and authorize the credentials of the individual requesting the collation and analysis. BT.6.13. Provide a mechanism to label the resultant information with appropriate privacy policy constraints and categorizations.

Technical Requirement Category	Identity Credentials (1) (User Categories, Purpose Metadata)	Electronic Policy Rules (2) (Conditions, Obligations Metadata)	Content Metadata (Data Categories, Purpose Metadata)	PDP/PEP (3) (Actions, Obligations Metadata)
	BT.6.12b. Provide a mechanism to authenticate and authorize the credentials of the individual requesting the collation and analysis.	BT.6.21. Provide mechanisms to express prerequisites for merging. BT.6.22. Include confirmation that two sources of information address the same individual/organization.		BT.6.23. Provide mechanisms to block merging if prerequisites are not met or included metadata about the possibility of the match not being accurate.
BT.7.0x Sharing and Disclosure of Information	BT.7.11. Define subject names for the appropriate user group and role associations to name in the policy.	BT.7.13a. Describe the circumstances under which to accept or deny a request to access information based on user group/role and purpose.	BT.7.12a. Provide the ability to associate law enforcement, public protection, public prosecution, public health, and justice purpose with information.	BT.7.12b. Provide the ability to gather information at the time of request as to the law enforcement, public protection, public prosecution, public health, and justice purpose with an access request. BT.7.13b. Provide the ability to accept or deny a request to access information based on user group, role, and purpose. BT.7.14. Maintain an audit trail for access or dissemination.
	BT.7.21. Define subject names for the appropriate external user group and role associations to name in the policy.	BT.7.22. Same as BT.7.1x, items 1–4 above, but add "avoid imminent danger or certain danger to life or property" as a purpose and allow exceptions based on this purpose.		
		BT.7.31. Define "specific purposes" in a machine-readable form.	BT.7.32. Mark information to associate it with specific purposes.	BT.7.33. Positively identify individuals that have access to information under those purposes. BT.7.34. Enforce rules that release information under the specific purpose to authenticate.
			BT.7.41. Mark information as to whether it is accessible	BT.7.42. Enforce rules that govern the release of information

Technical Requirement Category	Identity Credentials (1) (User Categories, Purpose Metadata)	Electronic Policy Rules (2) (Conditions, Obligations Metadata)	Content Metadata (Data Categories, Purpose Metadata)	PDP/PEP (3) (Actions, Obligations Metadata)
			to the public.	to the public.
				BT.7.51. Positively identify individuals outside agency. BT.7.52. Accurately track information to subject and correlate with authenticated individual. BT.7.53. Enforce disclosure policy based on BT.7.4x, items 1–2.
BT.8.0x Information Retention and Destruction	BT.8.03a. Define credentials required to approve information retention and destruction.	BT.8.01a. Specify schedule for information review.	Include metadata relevant to retention period, for example, when data gathered and the retention period or category.	BT.8.01b. Set up schedule for information review. BT.8.02. Scan marked information and invoke actions. BT.8.03b. As required, seek approval before action. BT.8.04. As required, notify appropriate parties of action. BT.8.05. Record actions.
BT.9.0x Accountability and Enforcement		BT.9.11. Provide a means to satisfy requests from the public to access the policy.		
				BT.9.21. Implement information protection mechanisms that are consistent with applicable standards of benchmarks, for example, logging and audits.
				BT.9.31. Implement restrictions specified in enforcement policy (e.g., identify suspended or demoted individual and block access as appropriate).

Notes:

1. The requirements under "Identity Credentials" provide input to user category metadata models (in EPAL terminology).
2. The requirements under "Electronic Policy Rules" provide input to condition and obligation metadata models (in EPAL terminology).
3. The requirements under "PDP/PEP" provide input to action and obligation metadata models (in EPAL terminology).

Note: We assume that "release" or disclose" may include the following possible outcomes:

- Disclosure of all of the information or documents requested without redaction.
- Disclosure of selected pieces of information or portions of documents.
- Disclosure of some or all of the information requested with associated handling criteria regarding use of the information, qualifications regarding the meaning of the information disclosed, or limitations on further disclosure (i.e., obligations).
- Disclosure of anonymized information.
- Disclosure of a statistical report or other summary of compiled information.
- No disclosure of information itself, but indication that there is an officer safety issue regarding the person about whom information was sought.
- No disclosure of any information initially, with referral of the request to a person who will decide what information to disclose, if any.
- No disclosure of information itself—disclosure of the existence of information and invitation to the requestor to come to originating agency to view the information.
- No disclosure of information itself—disclosure of the existence of information and refer the requestor to an identified individual in originating agency.
- No disclosure of information itself with notification to a specific individual (for example, investigating officer) at originating agency that an inquiry was made ("silent hit").
- No disclosure of any information, existence of information, or notification of anyone in the originating agency of the request.

Appendix C: Sample Privacy Policy Analysis

We selected a sample section at random from readily available justice community policy documents. Our sample is drawn from the *California Criminal Record Security: Statutes and Regulations*, dated August 2003. It is entitled "Access to Information" (page 50 of the document). This section is replicated below. The policy addresses the release of "criminal offender record information" and, in particular, when the subject of that information is a "peace officer or applicant for a position as a peace officer." Our analysis proceeds paragraph-by-paragraph through the policy and identifies the role of the applicable technical framework components and Appendix B requirements in implementing each paragraph.

ACCESS TO INFORMATION

13200. Right of authorized access to individual record information not affected

Nothing in this chapter shall be construed to affect the right of access of any person or public agency to individual criminal offender record information that is authorized by any other provision of law.

13201. Access to individual record information only if authorized by law

Nothing in this chapter shall be construed to authorize access of any person or public agency to individual criminal offender record information unless such access is otherwise authorized by law.

13202. Public agencies and research bodies; access to criminal offender record information; removal of individual identification; costs

Every public agency or bona fide research body immediately concerned with the prevention or control of crime, the quality of criminal justice, or the custody or correction of offenders may be provided with such criminal offender record information as is required for the performance of its duties, provided that any material identifying individuals is not transferred, revealed, or used for other than research or statistical activities and reports or publications derived there from do not identify specific individuals, and provided that such agency or body pays the cost of the processing of such data as determined by the Attorney General.

13203. Arrest or detention of peace officer; post-arrest diversion programs; release of Information

(a)Any criminal justice agency may release, within five years of the arrest, information concerning an arrest or detention of a peace officer or applicant for a position as a peace officer, as defined in Section 830, which did not result in conviction, and for which the person did not complete a post-arrest diversion program, to a government agency employer of that peace officer or applicant.

(b)Any criminal justice agency may release information concerning an arrest of a peace officer or applicant for a position as a peace officer, as defined in Section 830, which did not result in conviction but for which the person completed a post-arrest diversion program or a deferred entry of judgment program, or information concerning a referral to and participation in any post-arrest diversion program or a deferred entry of judgment program to a government agency employer of that peace officer or applicant.

(c)Notwithstanding subdivision (a) or (b), a criminal justice agency shall not release information under the following circumstances:

(1) Information concerning an arrest for which diversion or deferred entry of judgment has been ordered without attempting to determine whether diversion or a deferred entry of judgment program has been successfully completed.

(2) Information concerning an arrest or detention followed by a dismissal or release without attempting to determine whether the individual was exonerated.

(3) Information concerning an arrest without a disposition without attempting to determine whether diversion or a deferred entry of judgment program has been successfully completed or the individual was exonerated.

13200. Right of authorized access to individual record information not affected

Nothing in this chapter shall be construed to affect the right of access of any person or public agency to individual criminal offender record information that is authorized by any other provision of law.

13201. Access to individual record information only if authorized by law

Nothing in this chapter shall be construed to authorize access of any person or public agency to individual criminal offender record information unless such access is otherwise authorized by law.

Component	Requirement	Analysis
Electronic Policy Statement	BT.2.01	These two introductory paragraphs defer the policies to other applicable provisions of law. BT.2.01 requires that the Electronic Policy Statement capture the implication of compliance with the law. This policy statement invokes the requirement to support a hierarchical relationship among electronic policy statements by allowing the policy itself to be overridden by law.
Content Metadata	BT.3.01, BT.4.1x	Consistent with the referenced requirements, information must be marked as *criminal offender information* in order to enforce the provisions of this policy.

> ***13202. Public agencies and research bodies; access to criminal offender records information; removal of individual identification; costs***
>
> *Every public agency or bona fide research body immediately concerned with the prevention or control of crime, the quality of criminal justice, or the custody or correction of offenders may be provided with such criminal offender record information as is required for the performance of its duties, provided that any material identifying individuals is not transferred, revealed, or used for other than research or statistical activities and reports or publications derived there from do not identify specific individuals, and provided that such agency or body pays the cost of the processing of such data as determined by the Attorney General.*

Component	Requirement	Analysis
Credentials	BT.7.11, BT.7.21	Implementing this paragraph requires credentialing "Every public agency or bona fide research body immediately concerned with the prevention or control of crime, the quality of criminal justice, or the custody or correction of offenders." There will most likely be a list of organizations that meet this criteria, and individuals will be credentialed as members of the organizations; for example, if media organizations or academic institutions meet this criteria, individuals will be credentialed as members of the organizations. However, some requests will be ad hoc and may require human review to "credential" the organization and its authorized members.
Electronic Policy Statement	BT.7.13a	The electronic policy must reflect that information is to be released only to individuals or agencies identified above under the condition that "any material identifying individuals is not transferred, revealed, or used for other than research or statistical activities and reports or publications derived there from do not identify specific individuals."
Content Metadata	BT.3.01, BT.4.1x	As with the first two paragraphs, it is a requirement to label data as "criminal offender record information as is required for the performance of its duties."
PDP/PEP	BT.7.13b	The PDP/PEP enforces this release policy, although the requirement to pay for information is probably out of scope of framework and would be implemented by other software applications.
Obligation Metadata		Pass along a requirement to the requestor that "any material identifying individuals is not transferred, revealed, or used for other than research or statistical activities and reports or publications derived there from do not identify specific individuals."

> ***13203. Arrest or detention of peace officers; post-arrest diversion programs; release of Information***
>
> *(a) Any criminal justice agency may release, within five years of the arrest, information concerning an arrest or detention of a peace officer or applicant for a position as a peace officer, as defined in Section 830, which did not result in conviction, and for which the person did not complete a post-arrest diversion program, to a government agency employer of that peace officer or applicant.*

Component	Requirement	Analysis
Credentials	BT.7.11, BT.7.21	The organization approved to receive the subject information is "a government agency employer of that peace officer or applicant." This type of agency needs to be credentialed accordingly.
Electronic Policy Statement	BT.7.13a	The electronic policy must reflect that information is to be released within the time periods and under the conditions (e.g., "did not result in conviction, and for which the person did not complete a post-arrest diversion program"). It must also check to ensure that the request is only regarding the employment or prospective employment of the officer or applicant. This policy statement may also constitute a requirement for an obligation.
Content Metadata	BT.3.01, BT.4.1x	It is a requirement to label data as "information concerning an arrest or detention." Also, the date of arrest is needed in order to know whether the 5-year limit applies.
PDP/PEP	BT.7.13b	The PDP/PEP enforces this release policy.
Obligation Metadata		By implication, the agency receiving this information may not disclose it to a third party.

> ***13203. Arrest or detention of peace officers; post-arrest diversion programs; release of Information***
>
> *(b) Any criminal justice agency may release information concerning an arrest of a peace officer or applicant for a position as a peace officer, as defined in Section 830, which did not result in conviction but for which the person completed a post-arrest diversion program or a deferred entry of judgment program, or information concerning a referral to and participation in any post-arrest diversion program or a deferred entry of judgment program to a government agency employer of that peace officer or applicant.*

Component	Requirement	Analysis
Credentials	BT.7.11	In this situation, the party receiving the information is not specified. This is an example of an ambiguity in the law that needs to be resolved by policymakers before it can be implemented electronically.
Electronic Policy Statement	BT.7.13a	The electronic policy must reflect that information is to be released within under the conditions specified (e.g., "completed a post-arrest diversion program or a deferred entry of judgment program, or information concerning a referral to and participation in any post-arrest diversion program or a deferred entry of judgment program to a government agency employer of that peace officer or applicant").
Content Metadata	BT.3.01, BT.4.1x	It is a requirement to label data as "information concerning an arrest." The fact that the "information concerning an arrest" is associated with a peace officer may be obtained by examining the credentials of the subject. The detail that the subject has "completed a post-arrest diversion program or a deferred entry of judgment program, or information concerning a referral to and participation in any post-arrest diversion program or a deferred entry of judgment program to a government agency employer of that peace officer or applicant" will need to be kept with or associated with the arrest information.
PDP/PEP	BT.7.13b	The PDP/PEP enforces this release policy.

The above analysis validates that the requirements are sufficient to address the automation of a sample real-life policy.

Appendix D: Privacy Policy Metadata Elements

For a comprehensive discussion of the privacy policy metadata elements, please review:

http://www.privacywiki.org/index.php/Privacy_Policy_Metadata_Requirements

This appendix describes a framework of metadata elements that provide a vocabulary for the definition and enforcement of privacy policies in a justice information sharing environment.

1. Definitions

The following terms and definitions are used frequently in this Appendix:

- *Requestor*—The person requesting information about the *subject*.
- *Source*—The person who initially gathered the information about the *subject*.
- *Source agency*—The organization on whose behalf the *source* initially gathered the information about the *subject*.
- *Subject*—The person or organization about whom information is directly or indirectly requested and whose privacy, civil rights, and civil liberties must be protected.
- *Submitter*—The person responsible for making the data about the *subject* available.
- *Submitting agency*—The agency on whose behalf the *submitter* made the information about the *subject* available.

2. Content Metadata

Content metadata describes properties of the information being exchanged or to be exchanged. Content metadata includes the following groups of metadata elements:

- Data Category Metadata
- Purpose Metadata

2.1. Data Category Metadata

Data category metadata describes properties of the data, including data type categories, associations of the data with persons and organizations, data classifications, and data quality information. These include:

- Data Type Category Metadata
- Association Metadata
- Data Classification Metadata
- Data Quality Metadata
- Source Metadata

2.1.1 Data Type Category Metadata

Data type categories are high-level groupings of data, such as contact information, medical records, or criminal records. These categories are used to distinguish groups of collected data that need to be treated differently from a privacy point of view. Organizing the data categories into a hierarchy improves the expressiveness of rules.

Data Type Category Metadata Elements

Data type category is described with the following metadata element:

- **Data type category**—groupings of data that have different privacy requirements.

Data Type Category Metadata Code List

Value	Description
Behavioral	Behavioral information includes anything a person does, including hobbies and activities.
Contact	Contact information, including names, aliases, nicknames, home addresses, phone numbers, and e-mail addresses.
Criminal	Criminal record information, including arrests, charges, court judgments and sentences, and corrections.
Demographic	Demographic classifications, including race, religion, and sexual orientation.
Education	Educational background, including schools attended, degrees received, and skills acquired.
Employment	Employment background, including past and current employers, employer contact information, job titles, and dates of service.

Financial	Financial information, including bank accounts and balances and stock holdings.
Government	Government-issued identifiers, including tax identifiers and drivers license numbers.
Health	Health information, including past and current medical and psychological conditions, healthcare providers, treatments, prognosis, and DNA.
Identifiers	Nonfinancial, nongovernmental identifiers, including customer numbers, order numbers, and user identifiers.
Juvenile	Juvenile/child records, including incidents, court findings, custodies, and treatments.
Location	Physical location where the person has been or currently is located. This is distinct from his/her home or work addresses.
Other	Information that is not appropriate to one of the other categories.
Organizational	Known member of an organization.
Physical	Physical description information, including images, dental records, biometrics, and scars/marks/tattoos.
Political	Political preferences, including party affiliations.
Property	Any personal property that is fully or partially owned by the individual, including real estate and vehicles.
Proprietary	Proprietary information including trade secrets.
Reference	List of other databases that may have more information related to this information.
Sealed	Any information that has been sealed or expunged by a court.

2.1.2 Association Metadata

Association metadata describes privacy-related associations between a *subject* and other persons or organizations. For instance, attorneys may have access to certain private information about their client.

Association Metadata Elements

There are many possible associations between a *subject* and other persons and organizations. Therefore, we do not attempt to provide a comprehensive list in this document. However, many of the important relationships in a justice information sharing exchange can be described through an "Affiliation" association that indicates that the *subject* is a known member of a certain organization.

2.1.3 Data Classification Metadata

Data classification metadata describes the level of authorization required to view certain data. Classifications are most appropriate to authorization and access control. However, privacy policies may make exceptions for certain classifications for reasons of national security or counterterrorism.

Data Classification Metadata Elements

The following element is adapted from the Criminal Information Sharing Alliance network (CISAnet) categories:

- **Data classification**—the level of authorization required to view data.

Data Classification Metadata Code List

Value	Description
Commercial	Information available by subscription from nongovernmental organizations (e.g., ChoicePoint, LexisNexis, Accurint, Dallas Computer).
Counter-Terrorism	Counterterrorism data and documents (e.g., CISAnet Document Repository).
Criminal Intelligence	Criminal intelligence data and documents covered by 28 CFR Part 23 (e.g., Criminal Law Enforcement Reporting and Information System [CLERIS], ACISS Systems, Regional Information Sharing Systems [RISS], Joint Regional Information Exchange System [JRIES], Law Enforcement Intelligence Unit [LEIU], Automated Criminal Intelligence Index [ACII]).
Criminal Investigative	Criminal investigative data and documents (e.g., CLERIS, Criminal Investigation Management System [CIMS], International Criminal Court [ICC]).
Criminal Justice	Law enforcement, courts, and correction information, mostly public record (e.g., wants/warrants, Nlets—The International Justice and Public Safety Network, records management system/computer-aided dispatch [RMS/CAD], sex offenders, parole/probation, concealed handgun permits, court dockets).
Criminal History	Criminal history data and documents covered by guidelines set forth by the National Crime Information Center (NCIC) (e.g., NCIC Criminal History).

Government	Other government records (e.g., tax data, labor data, Uniform Commercial Code [UCC] filings, property records, departments of motor vehicles, driver's licenses, boat ownership).
Public	Information that is available to the general public. (e.g., public Web sites, libraries, newspapers).
Support	Test data typically created for development and training. (e.g., test databases, test records in other operational data sources).

2.1.4 Data Quality Metadata

Data quality metadata describes the reliability and validity of the information. Privacy policies may restrict collection of or access to information that is unreliable or invalid.

Data Quality Metadata Elements

The following data quality metadata elements are adapted from the *Statewide Intelligence System Sample Operating Policies and Procedures*:[3]

- **Source reliability**—the reliability of the source of the information.
- **Content validity**—an index of the accuracy or truth of the information.

Source Reliability Metadata Code List

Value	Description
Reliable	The reliability of the *source* is unquestioned or has been well tested in the past.
Usually reliable	The reliability of the *source* can usually be relied upon. The majority of the information provided in the past has proved to be reliable.
Unreliable	The reliability of the *source* has been sporadic in the past.
Unknown	The reliability of the *source* cannot be judged; authenticity or trustworthiness has not yet been determined by either experience or investigation.

Content Validity Metadata Code List

Value	Description
Confirmed	The information has been corroborated by an investigator or another reliable independent source.
Probable	The information is consistent with past accounts.
Doubtful	The information is inconsistent with past accounts.
Cannot be judged	The information cannot be judged. Its authenticity has not yet been determined by either experience or investigation.

[3]See http://www.iir.com/28cfr/SampleOperatingPolicies.pdf.

2.1.5 Source Metadata

Source metadata describes the origin of the data and includes the following independent metadata elements. The elements in italics are defined in the Definitions section of this Appendix.

Source Metadata Elements

The *source* of information is described with the following metadata elements:

- ***Source***
- ***Source agency***
- ***Subject***
- ***Submitter***
- ***Submitting agency***
- **Source date**—date (and optionally time) the information about the subject was gathered by the source.
- **Submittal date**—date (and optionally time) the information about the subject was made available for sharing.

2.2 Purpose Metadata

Purpose metadata describes the business purposes for which private data was originally collected. This metadata may also be context metadata used in a request to identify the business purposes for which the information will be used.

Purpose Metadata Elements

The purpose of information exchange is described with the following metadata elements:

- **Business purpose**—a general category of business purpose for which the information was collected or will be used.
- **Justice-specific purpose**—a justice-specific business purpose for which the information was collected or will be used.

Business Purpose Metadata Code List

The primary code list for business purposes comes from the lines of business (LoBs) defined in the Federal Enterprise Architecture Business Reference Model.

Justice-Specific Purpose Metadata Code List

Value	Description
Identifying subjects	The information will be collected or used for the identification of a *subject* in a criminal investigation.
Officer safety	The information will be collected or used for the purpose of ensuring the safety of law enforcement officers.
Other purpose	Any other justice-specific business purpose.

3. Context Metadata

Context metadata describes the properties of the *requestor* and the *subject* at the time of the request, the reason for the request, and the restrictions on the use of the information. Context metadata includes the following groups of elements:

- User Category Metadata
- Condition Metadata
- Obligation Metadata
- Purpose Metadata
- Action Metadata

3.1 User Category Metadata

User category metadata represents the category of metadata defined properties (attributes) about *requestors* who potentially access private data. These properties can be used to classify *requestors* (e.g., role) and/or are used to make dissemination decisions regarding certain pieces of data.

User Information and Identifier Metadata Elements

The *requestor* is described with the following metadata elements:

- **Name**—the name of the requestor.
- **Organizational affiliations**—the organizations with which the requestor is affiliated, including their employer.
- **Contact information**—the address, phone, and/or e-mail address of the requestor.
- **Title**—the job title of the requestor.
- **Level of government**—the level of government that employs the requestor (e.g., federal, state, county, or municipal).
- **Requestor role(s)**—the role(s) of the requestor at his/her employer.

- **Requestor rights**—the rights and privileges of the requestor at his/her employer.

Requestor Roles Metadata Code List

Code Table	Value
Public Safety and Protection Roles	Sworn law enforcement officer
	Law enforcement investigator
	Public safety (fire, emergency medical services)
	Child protection
	Public health
	Mental health
	Traffic safety
Justice Roles	Attorney
	Prosecutor
	Clerk/court administrator
	Judge
	Victim
	Court support agencies (e.g., drug-testing labs)
Supervision Roles	Classification staff
	Corrections officer
	Medical personnel
	Parole/probation officer
	Diversion programs
Other Roles	Media
	General public

Requestor Rights Metadata Code List

Code Table	Value
National Security	Secret security clearance
	Top secret security clearance
	Top secret/special background security clearance
	Confidential security clearance
Criminal Justice	Certified 28 CFR
	Certified NCIC criminal history
	Certified NCIC hotfile
	Certified FBI Integrated Automated Fingerprint Identification System
	Certified FBI Integrated Identification Index (III)
	Certified National Instant Criminal Background Check System (NICS) file
Professional Licenses	Licensed clinical social worker
	Marriage, family, and child counselor (MFCC)
	Medical licenses

3.2. Condition Metadata

Conditions are expressions that evaluate the context of a request for data and determine whether the information can be shared (e.g., the *subject* must be in detention, the user category must be law enforcement).

Condition Metadata Elements

Factors that must be satisfied for information sharing are described in the following metadata elements:

- **JIEM process**—represents the status of the subject at the time of the request as defined by the Justice Information Exchange Model (JIEM) reference model.
- **JIEM condition**—the content of an exchange as defined by the JIEM reference model.
- **Other conditions**—other processes and conditions not defined by the JIEM reference model.

JIEM Process Metadata Code List

Value	Description
Investigation	Law enforcement and prosecutor activities preparing for filing of a case.
At Large	*Subject* is being sought, but is not in custody.
Detention	Pretrial detention of *subject* to guarantee appearance in court.
Pre-disposition Court	Court-related processes from filing to disposition.
Pre-disposition Supervision	Supervision of *subject* prior to case disposition.
Post-disposition Court	Court events occurring after disposition.
Post-disposition Supervision	Supervision of *subject* following court disposition.
Incarceration	*Subject* in custody as sentenced by court.

JIEM Condition Metadata Code List

The list of conditions defined in the JIEM reference model is extensive and is not included here. However, the list of JIEM conditions is not comprehensive. Additional conditions must be defined using the Other Conditions element.

3.3 Obligation Metadata

Legislation and privacy policies may state that when a certain action is performed, the enterprise is obligated to take some additional steps. Examples of obligation metadata are that all accesses against a certain type of data for a given purpose must be logged or that certain data shall be deleted within 30 days.

Obligation Metadata Elements

Obligations associated with an information exchange are described with the following metadata elements:

- **Retention**—rules regarding the keeping of shared information for particular purposes and deletion after a specified time.
- **Dissemination**—rules regarding the distribution of shared information with other parties.
- **Audit**—rules regarding the logging of dissemination of shared information.
- **Notification**—rules regarding the notification of parties that information has been disseminated.
- **Other obligations**—other rules not covered by the obligation metadata defined above.

Retention Metadata Code List

Value	Description
No retention	Information is not retained for more than a brief period of time necessary to make use of it during the course of a single online interaction.
Stated purpose	Information is retained to meet the stated purpose. This requires information to be discarded at the earliest time possible.
Legal requirement	Information is retained to meet a stated purpose, but the retention period is longer because of a legal requirement or liability. For example, a law may affirmatively require a certain agency to maintain records for auditing or other soundness purposes. For example, 28 CFR Part 23 requires either revalidation or deletion of information after five years.
Business practices	Information is retained under a service provider's stated business practices.
Indefinitely	Information is retained for an indeterminate period of time. The absence of a retention policy would be reflected under this option.

Dissemination Metadata Code List

Value	Description
No dissemination	The *requestor* may not share or disseminate the information with anyone. An example would be criminal convictions that have been expunged.
Limited dissemination	The *requestor* may share the information with certain groups, for example, other law enforcement personnel involved in the investigation or activity, but may not share or disseminate the information to others, in particular, the public.
No limitation	The *requestor* may share the information without limitation.

Audit Metadata Code List

Value	Description
No auditing required	The *requestor* is not required to keep a log of the sharing of use of the information.
Auditing required	The *requestor's* agency must maintain an audit log of those with whom the information is shared.

3.4. Purpose Metadata

The content metadata for describing the business purpose for which information was collected may also be used as context metadata in a request to identify the business purposes for which the information will be used. The code list for both the content and context uses is described in the content Purpose Metadata section.

3.5. Action Metadata

Action metadata identifies the type of access the requestor would have to the data. Privacy rules typically define whether a requestor can perform the "read" action on the data. However, a framework intended to support security must also govern other types of actions, including "create," "update," and "delete."

Action Metadata Code List

Value	Description
Create	The *requestor* may insert a new record or data element.
Read	The *requestor* may read a record or data element.
Update	The *requestor* may update a record or data element.
Delete	The *requestor* may delete a record or data element.

4. Decision Metadata

The context and content metadata are parameters used in making the decision of how to respond to a request for information. The result of the decision is described in the following groups of metadata elements:

- **Outcome metadata**
- **Notification metadata**

4.1 Outcome Metadata

Outcome metadata directs the system responding to the information sharing request as to what to do with the requested information. This metadata addresses how much of the information to disclose.

Outcome Metadata Elements

The actions resulting from an information sharing decision are described with the following metadata:

- **Outcome**
- **Redaction type**

Outcome Metadata Code List

Value	Description
Disclose	Disclose the requested information in its entirety.
Redact	Disclose some of the requested information and redact certain information according to one or more redaction types.
Deny	Do not disclose any of the requested information.

Redaction Type Metadata Code List

Value	Description
Classified information	All information with a national security classification level must be redacted.
Confidential sources	All information received from confidential informants or other secret sources must be redacted.
Open cases/ongoing investigations	All information pertaining to open criminal court cases or ongoing law enforcement investigations must be redacted.
Personally identifiable information (PII)	All information that can be used to individually identify a person must be redacted.
Sealed court cases	All information that is sealed by a court must be redacted.

4.2 Notification Metadata

There are a number of situations in justice information sharing in which requests for certain types of information must be reported to a third party. If there is a requirement that someone be notified of a request, notification metadata identifies the person to be notified to the system responding to the information sharing request.

Notification Metadata Elements

The notification requirements resulting from an information sharing decision are described with the following metadata:

- **Notification type**—an individual to notify of the request.
- **Notified person contact information**—the contact information for the individual to notify.
- **Notified organization**—the organization that the individual to be notified represents.
- **Notified person role**—the role of the individual to notify.

Notification Type Metadata Code List

Value	Description
Subject	Notify the *subject* of the information.
Submitter	Notify the *submitter* of the information.
Supervisor	Notify the supervisor of the *subject*.
Subscriber	Notify an individual that has subscribed to watch the information (silent hits).

5. References

Global Privacy and Information Quality Working Group, *Information Quality: The Foundation for Justice Decision Making.* Retrieved from http://it.ojp.gov/documents/IQ_Fact_Sheet_Final.pdf.

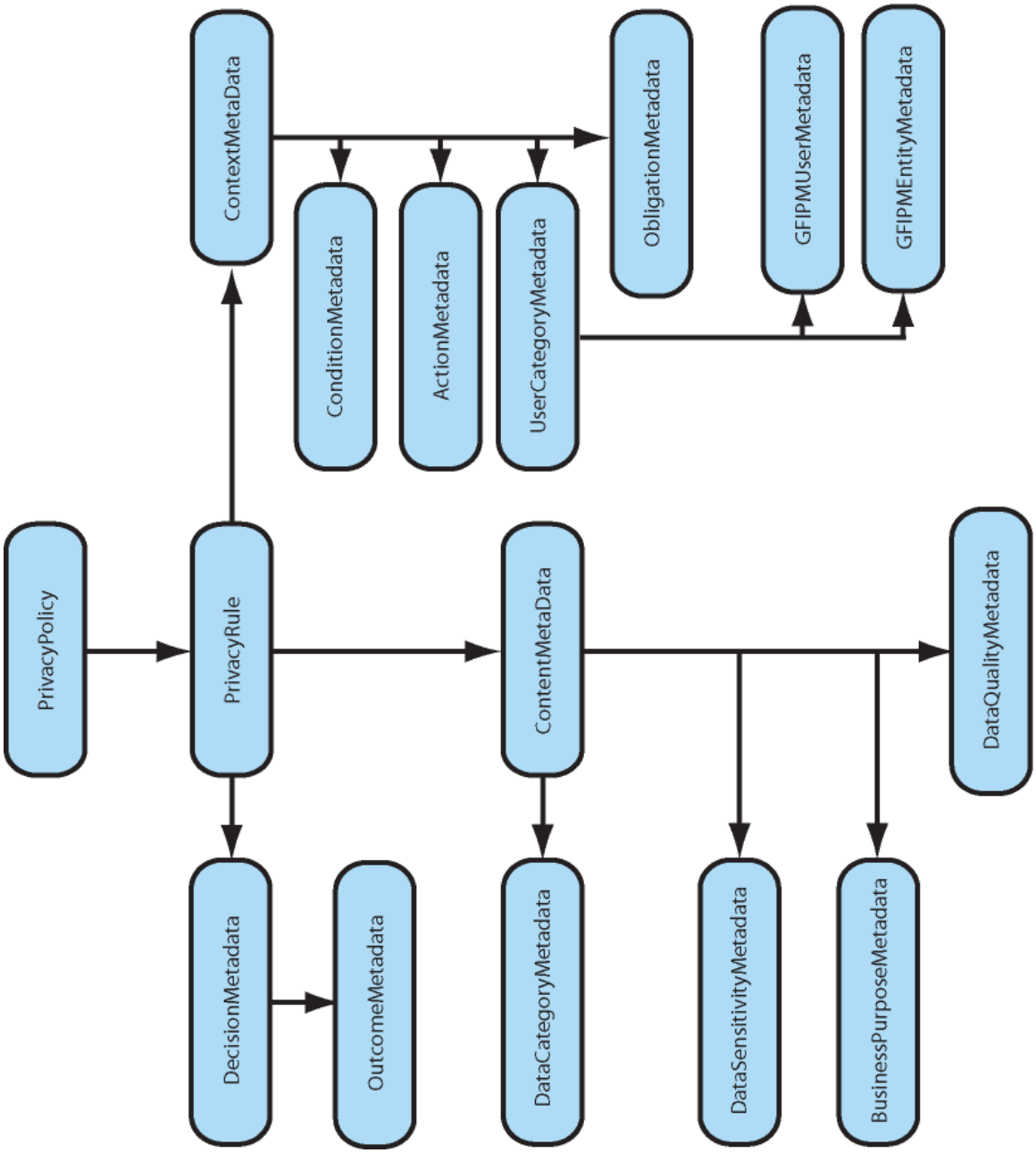


Figure 12: Privacy Policy Metadata Model

Appendix E: Assessment of Current and Emerging Technologies Relating to Privacy

This section highlights the various commercial products that currently exist and are advertised to support various components of the Privacy Policy Technical Framework discussed in this report. The list is not exhaustive, and under no circumstances should any of these product summaries be construed as a product endorsement. They are listed to provide the reader with starting points for evaluating best-fit hardware/software investments for their enterprise policy services strategy.

The broad category of terms under which these vendor offerings are catalogued includes user provisioning tools, service-oriented architecture (SOA) management services software, user entitlement software, advanced identity and access management software, XML Security software, role-based access control software, audit and logging software, policy services, and authorization services.

Vendor packaging includes these product modules in their SOA registry product suites, application vendor suites, stand-alone security or policy-focused vendors, and XML Security appliances.

The review was focused on functionality of products and not focused on justice-specific products. The area of fine-grained authorization services is still in the early stages of maturity and will undergo a variety of growing pains before being considered a mainstream product set.

The demand for greater privacy protections, identity theft, and a heightened awareness of the need to exchange confidential information in the justice domain will continue to drive accelerated growth and development of policy software products for many years to come.

The following is a sample listing of technical software alternatives for implementing privacy policy.

1. Products, Platforms, and Frameworks

This section highlights the various commercial products that currently exist and are advertised to support various components of the Privacy Policy Technical Framework discussed in this report. The list is not exhaustive, and under no circumstances should any of these product summaries be construed as a product endorsement. They are listed to provide the reader with starting points for evaluating best-fit hardware and software investments for their enterprise policy services strategy.

1.2. Application Vendor Suites

1.2.1 Tivoli Access Manager (IBM)

The Tivoli Access Manager is a security management product that is geared towards the access control of resources, authentication of users, and the application and development of policies. Much of the access manager implementation is based on the notion of users, groups, and roles with permissions being granted to resources. To some extent, there are limitations to the granularity of the resources to which the policies are applied.

The policy authoring is done via proprietary mechanisms within the access manager and does not support natural language policy authoring. Much of the Tivoli Policy Manager functionality can be accomplished in Tivoli Access Manager. Two inadequacies of the program are the loss of granularity of the auditing capability and the natural language creation of policies.

It is suspected that the Server Privacy ARchitecture and CapabiLity Enablement (SPARCLE) research project is intended to provide a Privacy Manager and also provide a more comprehensive Privacy/Entitlement Management offering that will complement WebSphere.

		Notes
Natural Language Authoring	No	
PAP		
Authoring Application	Yes	GUI-based application
Policy Definition Language	Yes	Proprietary
Import/Export Capability	No	
Fine Granularity	No	
Obligation Support		
Auditing		
PDP		
Auditing		

1.2.2. AquaLogic Enterprise Security (BEA)

AquaLogic Enterprise Security is a component of the AquaLogic family of products from BEA.[4] It is a distributed architecture entitlements management solution that integrates with both the BEA AquaLogic and BEA WebLogic suites and consists of a PDP and PAP.

The PDP performs both decision and enforcement capability. It can either be centralized as a Web service or distributed at individual application servers using Security Service Modules

[4] BEA AquaLogic Enterprise Security, "Managing Entitlements—The Next Phase of Application Security," Revised December 2006, see BEA AquaLogic Enterprise Security.

(SSM). SSMs are platform-specific plug-ins and are available for most Microsoft and Java platforms.

The Policy Administration Server defines the policy and security configurations via an administrative console. The console is also exposed as a Web application. Three types of policies are supported:

- Role-mapping policies, that are used to define rules about users' roles.
- Access policies, which control access to both application software components and application business data objects.
- Delegation policies, which enable delegation of policy management.

The policies are managed with a predefined syntax that is not natural language-based. Policies created via the GUI are expressed with XACML 2.0 support. When used in conjunction with Web services, the XACML is transported using SAML 1.1.

1.3. Stand-Alone Security or Policy-Focused Vendors

1.3.1 Entitlement Manager (Securent)

The Securent Entitlement Manager is presented as a complete entitlement management solution that consists of a PAP, PEP, and PDP.

It is a distributed application that relies on Web services for all pieces of its implementation and uses XACML 2.0 and SAML 2.0 to convey the relevant information in SOAP messages. The basic design is to be platform-independent. The PEP has built-in support for use with some products and requires custom coding for the remainder. It currently has explicit support for IBM WebSphere, BEA WebLogic (now AquaLogic), MS Sharepoint, and JBOSS.

The PEP plugs into security application program interfaces to expose the relevant resources for applying policy via Policy Administration Point (PAP). The solution uses a Web-based portal for access to the PAP for policy authoring. The portal uses a drag-and-drop GUI to graphically define the policy, which is then rendered into XACML. Again, the limitations of what can have policies applied to it are limited by the PEP plug-ins that it uses. Anything finer-grained than what is available out-of-the-box requires custom coding.

1.3.2 Embedded Entitlements Manager (CA)

The CA Embedded Entitlements Manager is another complete solution for managing entitlements. Architecturally, the functionality is split between the Entitlements Management Server and the Embedded Entitlements Manager software development kit (SDK).

Functionally, the CA Embedded Entitlements Manager is similar to the Securent Entitlement Manager.

The Entitlements Manager Server hosts both the PEP and the policy authoring and management. It is managed to a completely Web-based GUI. The ability to author the policies is dependent on the exposure of resources via the Embedded Entitlements Manager SDK. All policies that are authored are rendered into XACML and transported via SAML. All authored policies are externally visible.

The Embedded Entitlements Manager SDK is a software development kit that requires coding. The SDK itself is available for both Java and .NET platforms and allows for the exposure for resources to the Entitlements Manager Server and also implements the means for the PDP code to be executed from the client software.

1.3.3 Aveska, NetVision, SailPoint

These vendors are addressing the Identity Risk Management and compliance portion of policy auditing and monitoring. The products analyze scope of user entitlements, activity logs, and risk levels of the resources the identities access to monitor compliance and identify high-risk activity or high-risk modifications to access (entitlement) privileges.

1.3.4 Vontu 7 (Vontu)

Vontu 7 is a strictly data-centric approach to protection of data. The product is organized into three basic categories concerning information sharing:

- "Data at Rest" represents data at the originating database or computer.
- "Data in Motion" represents data traversing the network.
- "Data at the Endpoint" represents data at a destination computer or database.

In the context of this product, data protection refers to ensuring that only those people who are allowed to see specific types of data are granted access. Functionally, it is the same as any other means of ensuring privacy of data.

Regardless of which category described above the data fits into, the application of privacy protection is the same. The product supports the ability to author and deploy policies and also provides the administrative capability for managing the enforcement and metrics of those policies at differing levels. Policy authoring is managed via a proprietary GUI and applies policies to data that needs to be protected by "indexing" the critical data. The indices can be considered metadata to some extent. The indexing hashes and copies the data internally. The policies are proprietary in nature and cannot be imported or exported.

Enforcement is managed by comparison of the data being manipulated with the hashed stored data that has been indexed. Depending on the policy, the access to the data can be denied or flags raised for notification. The enforcement and metrics capabilities supporting accountability are very robust and are accessible via the same GUI from which policies are authored.

1.3.5 Elemental Security Platform (Elemental Security)

The Elemental Security Platform is a complete security platform that contains a policy deployment and enforcement framework. There is no real available data on how it works, although terminology usage implies that policies are XACML-based. It does not have any policy-authoring capabilities but does contain much in the way of auditing and accountability support.

Most of the other areas of the platform focus on areas of role-based access control, such as RBACx.

1.3.6 RBACx (Vaau)

The RBACx is a security management product geared towards role-based access control using a role-based J2EE platform that manages the relationships between identities, policies, and business processes. It does not have the capability of defining or managing policies directly.

It is treated as an adjunct product to enhance the access control of products by IBM, BEA, Sun, and Microsoft.

1.4. SOA Registry Product Suites

1.4.1. Infrastructure Suite (SOA Software)

The SOA Software Infrastructure Suite is a comprehensive platform for all facets of an SOA system and covers the areas of policy management, governance, management, and security. It consists of two basic component areas, the Workbench and the Service Manager.

The Workbench serves as the PAP where metadata used for the application of policies is defined, stored, and registered and also implements the relevant workflow with which the policies will interact. Any authored policies are discoverable via UDDI, and the policies are not rendered as XACML.

The Service Manager implements the PDP and PEP and is responsible for the capture and dissemination of the auditing and usage metrics of the system.

2. New Technologies

This section highlights those known technologies and products that are in development or are very new. None of the items here can be considered to be very robust at this time and need to be scrutinized further.

2.1. Application Vendor Suite(s)

2.1.1. SPARCLE (IBM)

The Server Privacy ARchitecture and CapabiLity Enablement (SPARCLE) is a prototypical development product at IBM that is currently available on a limited basis with select users and projects. The primary focus is to use natural language (prose) for authoring policy to be used by enforcement engines.

Functionally, the user writes or types the policy in a semiformalized prose style. The prose is parsed and the platform extracts the key elements from the natural language policy and then generates XACML. Conversely, XACML policy can be read and reviewed in natural language. The policy output is portable and can be used in any enforcement engine supporting XACML.

The policy authoring is not limited to privacy and can also be used for policy confirmation and verification. It also has some form of auditing, but there are no details on that function at this point in time.

This prototype has been in development for two years and has gone through two iterations. A third iteration is due to be released sometime in the near future.

3. XML Appliances

There is widespread use of hardware-based technologies to accelerate the performance of certain time-intensive tasks in distributed processing environments. The hardware that is used to perform these time-intensive tasks can be referred to as appliances and can be used in several different ways. The following are some examples, but this is not an exhaustive list.

- Gateway provides security for the network but focuses on XML services.
- Accelerator speeds up the processing and transformation of XML on the network.
- Proxy provides a proxy for Web services inside the firewall.
- Hybrid “Plus” provides gateway, accelerator, and proxy, plus other functionality.

Note that in some respects, these do not really belong in a document of this type, but they are included for the purposes of illustrating that certain functions within a privacy framework could be augmented to improve performance requirements.

These appliances have been compared using information from a previous presentation given at the Nlets—The International Justice and Public Safety Network conference of January 2007. The tasks for comparison are listed as follows:

- Routing—Directing an incoming message to one or more destinations based on the contents of the message.
- Service Mapping—Mapping external Web services to internal views of those services within the appliance; acts as a proxy for a Web service.
- Protocol Transformation—Converting an incoming message with one format to an outgoing message of another format.
- Protocol Transformation Enhancement—The same as Protocol Transformation but with the ability to augment the outbound message with data not originally present or able to be inferred from the incoming message.
- Protocol Transformation Processing—To perform actual work based on the contents of the message in addition to transforming the results.
- Work Flow—The direction that the data moves through the process.
- Work Flow Choreography
- Service Orchestration

3.1. WebSphere DataPower Integration Appliance X150 (IBM)

There are three DataPower Appliances:

- Integration Appliance X150 (IBM)
- XML Accelerator XA35
- XML Security Gateway XS40

The tasks that they collectively can support are listed below:

Task	Availability	Notes
Routing	Yes	
Service Mapping	No	
Protocol Transformation		
Transformation	Yes	
Enhancement	Yes	
Processing	Yes	
Work Flow		
Process Choreography	No	
Service Orchestration	No	
Transaction Management	Yes	
Security	Yes	WS-Security 1.1, WS-Trust, SAML, and LDAP

3.2. XML VPN (Digital Evolution)

The XML VPN appliance offered by Digital Evolution supports the following tasks:

Task	Availability	Notes
Routing	No	
Service Mapping	Yes	Implements a proxy
Protocol Transformation		
Transformation	No	
Enhancement	No	
Processing	No	
Work Flow		
Process Choreography	No	
Service Orchestration	No	
Transaction Management	Yes	
Security	Yes	WS-Security 1.1, XML-Signature, and XML-Encryption

3.3 Reactivity XML Appliances (Reactivity)

Reactivity offers three different appliances: the XML Security Gateway for optimization service performance; the Secure XML Router, which accelerates routing and security; and the XML Accelerator, which performs XML message inspection, security, and access control.

Task	Availability	Notes
Routing	Yes	
Service Mapping	Yes	
Protocol Transformation		
Transformation	No	
Enhancement	No	
Processing	No	
Work Flow		
Process Choreography	No	
Service Orchestration	No	
Transaction Management	Yes	
Security	Yes	WS-Security 1.1, WS-Trust, SAML, and LDAP

3.4. XML Networking Gateway (Layer 7 Technologies)

Layer 7 Technologies offers an XML Accelerator, XML Data Screen, XML Firewall and VPN, and XML Networking Gateway that collectively support all of the following tasks.

Task	Availability	Notes
Routing	Yes	
Service Mapping	Yes	
Protocol Transformation		
Transformation	Yes	
Enhancement	No	
Processing	Yes	
Work Flow		
Process Choreography	No	
Service Orchestration	No	
Transaction Management	Yes	
Security	Yes	WS-Security 1.1 and SAML support. Custom policy SDK.

4. Other Technologies

The following products and initiatives are not consistent with the proposed technical framework in this report but do represent other policy efforts that readers will likely encounter in their review of policy implementation tools. These are included for completeness in describing the vendor landscape for developing privacy policy. These products are focused on end users' establishment of their own personal privacy preferences for interacting with various commercial Web sites versus our focus that is centered around the protection of personal information within the domain of justice information systems sharing. The other initiatives are not mainstream products for current adoption but represent some research and development areas within the industry.

4.1. Transparent Accountable Data Mining Initiative

Transparent Accountable Data Mining Initiative (TAMI) is an architecture which proposes a means for not only being able to implement the current and most immediate privacy requirements of today but which also proposes the means of ensuring that the usage of the information is not in violation of existing jurisdictional laws. Fundamentally, the architecture consists of three components:

- Inference Engine to support analysis of available data and assess compliance with policies.
- Truth Maintenance System for assessing reliability and recording justifications.
- Proof Generator to construct proofs showing that critical transitions and adverse uses of personal information are justified by facts and permissible under applicable rules.

The architecture uses resource description framework (RDF) and ontology Web language (OWL) because of the semantic support that is necessary for the inference to accurately take place. This architecture has been prototyped and proven successful, but it still requires additional research before it can be considered a viable approach.

4.2. Wisconsin Cascading Disclosure Control Language

In addition, the state of Wisconsin is pursuing a research and development project for implementing electronic policy for its justice information systems. The project is primarily focused on developing a user-friendly authoring tool for describing policy. The effort includes defining a custom PAL entitled Cascading Disclosure Control Language (CDCL).

4.3. CardSpace (Microsoft)

CardSpace (formerly InfoCard) is a Web-based identity management framework from Microsoft introduced with .NET 3.0 in the fourth quarter of 2006. It is based on the idea that any data being transmitted does not contain PII that could be used in determining the identity of a person. Instead of PII, metadata is used to specify a trusted third party that can truly identify the user.

The trusted third party issues a "user card" for use with Web applications. A user can have multiple cards issued from various authorities and chooses the one to be used for accessing a particular service. The service authenticates the card with the trusted third party.

This offering only applies to the identity management of users but introduces a different paradigm for ascertaining roles and how they relate to policy.

4.4. Security Policy Assertion Language (Microsoft Research)

Security Policy Assertion Language (secPAL) is a Microsoft Research project to develop a flexible and robust declarative security policy language to meet the access control requirements of large-scale Grid Computing Environments (GCE). See http://research.microsoft.com/projects/secpal. This PAL development project effort contains many of the same features and capabilities of the OASIS XACML standard.

4.5. Identity Governance Framework (Liberty Alliance)

The Identity Governance Framework (IGF)[5,6] is not a product but a proposed specification for managing identity and the application of policy to that identify. It was originally developed by Oracle and subsequently donated without intellectual property rights claim to Liberty Alliance for incorporation into its suite of security specifications.

The framework is meant to be able to adequately deal with applications accessing identity-related data and the definition, enforcement, and auditing or policies concerned with the use of identity-related data. The framework consists of four main components:

- The Identity Attribute Service—a service that allows access to identity sources and policy enforcement.
- Client Attribute Requirements Markup Language (CARML)—a declarative syntax for clients to specify the requirements for attributes.[7]
- Attribute Authority Policy Markup Language (AAPML)—an XACML 2.0 profile that dictates the policy on usage of information or data.[8]
- A client API for reading and writing identity-related attributes that can also act as an implementation guide.

IGF is still in its infancy; it was submitted to the Liberty Alliance in February 2007 as a royalty-free specification for standardization. The Liberty Alliance is in the process of forming a working group to be responsible for furthering this effort. This draft already has the support of many companies dealing with privacy.

It appears that the AAPML portion of the IGF may be similar to Microsoft CardSpace using identity metadata attributes, although this area will require additional research.

---

5 "Identity Governance Framework Frequently Asked Questions," November 29, 2006.
6 "Identity Governance Framework," an Oracle white paper, Phillip Hunt and Prateek Mishra, November 2006.
7 Client Attribute Requirements Markup Language (CARML) Specification, Working Draft 03, November 24, 2006.
8 AAPML: Attribute Authority Policy Markup Language, Working Draft 08, November 28, 2006.

Appendix F: Glossary

A

Access Control

The mechanisms for limiting access to certain information based on a user's identity and membership in various predefined groups. Access control can be mandatory, discretionary, or role-based.

Accountability Principle

One of the eight Fair Information Principles developed by the Organisation for Economic Co-operation and Development. According to this principle, a data controller should be accountable for complying with measures that give effect to the other seven principles.

Appropriate Security

An organization is required to take appropriate data security measures to protect personally identifiable information and prospect information. These measures must include physical security measures, such as doors and locks, as well as electronic security and managerial controls that limit the potential for unauthorized access or misuse by employees and contractors. The security measures necessary to protect information sufficiently will vary based on the risks presented to the individual by an organization's collection and use of the data.

Architecture

A set of artifacts (principles, guidelines, policies, models, standards, and processes) and the relationships between these artifacts that guide the selection, creation, and implementation of solutions aligned with business goals.

Awareness

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

Audit Trail

Audit trail is a generic term for recording (logging) a sequence of activities. In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms would record each user's activity in detail—what commands were issued to the system, what records and files were accessed or modified, etc. Audit trails are a fundamental part of computer security and are used to trace (albeit usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

Authentication

Authentication is the process of validating the credentials of a person, computer process, or device. Authentication requires that the person, process, or device making the request provide a credential that proves it is what or who it says it is. Common forms of credentials are digital certificates, digital signatures, smart cards, biometrics data, and a combination of user names and passwords.

Authorization

The process of granting a person, computer process, or device access to certain information, services, or functionality. Authorization is derived from the identity of the person, computer process, or device requesting access that is verified through authentication. See *Authentication*.

B

Behavior Model

The characterization of and responses to temporal dependencies between the actions on a service.

Business Process Models

A description (usually formal and often graphical) of a series of activities that culminate in the achievement of some outcome of business value. Some (but not necessarily all) of the steps in this series of activities involve producing a real-world effect provided by a capability, and some of the steps require a consumer to use a service. Each one of these steps provides the contextual justification for service interaction between a particular consumer and particular provider.

C

Capabilities

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

Collaboration

A capability that coordinates interaction with multiple services. A collaboration is often implemented using an open industry standard implementation mechanism that allows the implementation to be shared across tools and platforms.

Collection Limitation Principle

One of the eight Fair Information Principles developed by the Organisation for Economic Co-operation and Development. According to this principle, there should be limits to the collection of personal data, and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Confidentiality

Confidentiality is closely related to privacy but is not identical. It refers to the obligations of individuals and institutions to use information under their control appropriately once it has been disclosed to them. One observes rules of confidentiality out of respect for and to protect and preserve the privacy of others. See *Privacy*.

Consumer Systems

The information system that gains access to another partner's capability offered by means of a service.

Credentials

Credentials are information that includes identification and proof of identification that is used to gain access to local and network resources. Examples of credentials are user names, passwords, smart cards, and certificates.

D

Data

Inert symbols, signs, or measures.

Data Controller

A party who, according to domestic law, is competent to decide about the contents and use of personal data, regardless of whether or not such data is collected, stored, processed, or disseminated by that party or by an agent on its behalf.

Data Protection

Data protection encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, use, protection, and disclosure of information.

Disclosure

The release, transfer, provision of access to, or divulging of personally identifiable information in any other manner—electronic, verbal, or in writing—to an individual, agency, or organization outside of the agency who collected it.

Domain Vocabularies

Includes canonical data models, data dictionaries, and markup languages that standardize the meaning and structure of information for a domain. Domain vocabularies can improve the interoperability between consumer and provider systems by providing a neutral, common basis for structuring and assigning semantic meaning to information exchanged as part of service interaction. Domain vocabularies can usually be extended to address information needs specific to the service interaction or to the business partners integrating their systems.

E

Enforcement

A privacy principle that provides mechanisms for ensuring compliance with the Organisation for Economic Co-operation and Development's Fair Information Principles, recourse for individuals affected by noncompliance, and consequences for noncompliant organizations. Methods for enforcement include a review by independent third parties.

Enterprise Integration Patterns

Enterprise integration involves connecting multiple applications running on multiple platforms in different locations. Enterprise Integration Patterns help integration architects and developers design and implement integration solutions more rapidly and reliably. Most of the patterns assume a basic familiarity with messaging architectures. However, the patterns are not tied to a specific implementation.

Execution Context

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

F

Fair Information Principles (FIPs)

The Fair Information Principles are contained within the Organisation for Economic Co-operation and Development's "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data." These were developed around commercial transactions and the transborder exchange of information; however, they do provide a straightforward description of underlying privacy and information exchange principles, as well as a simple framework for the legal analysis that needs to be done with regard to privacy in integrated justice systems. Some of the individual principles may not apply in all instances of an integrated justice system.

The eight FIPs are:

- Collection Limitation Principle
- Data Quality Principle
- Purpose Specification Principle
- Use Limitation Principle
- Security Safeguards Principle
- Openness Principle
- Individual Participation Principle
- Accountability Principle

Framework

A set of assumptions, concepts, values, and practices that constitutes a way of viewing the current environment.

G

GJXDM

Global Justice Extensible Markup Language (XML) Data Model

Global

Global Justice Information Sharing Initiative

Global Justice Reference Architecture (JRA)

The Global JRA is an abstract framework for understanding significant components and the relationships between 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 Global JRA is being developed by Global; it leverages the work of others, such as the state of Washington, and builds upon the work of the Organization for the Advancement of Structured Information Standards (OASIS).

GUI

Graphical User Interface

H

Health Insurance Portability and Accountability Act (HIPAA)

A U.S. law that gives patients greater access to their own medical records and more control over how their personally identifiable information is used. The law also addresses the obligations of health care providers and health plans to protect health information. In general, covered entities—such as health plans, health care clearinghouses, and health care providers that conduct certain financial and administrative transactions electronically—had until April 14, 2003, to comply with this act.

I

IGF

Identity Governance Framework

Individual Participation Principle

One of the eight Fair Information Principles developed by the Organisation for Economic Co-operation and Development. As stated in the FIPs, according to this principle, an individual should have the right:

a) To obtain from the data controller or, otherwise, confirmation of whether or not the data controller has data relating to him;
b) To have communicated to him data relating to him:
   - Within a reasonable time
   - At a charge, if any, that is not excessive
   - In a reasonable manner
   - In a form that is readily intelligible to him
c) To be given reasons if a request made under subparagraphs a) and b) is denied and to be able to challenge such denial; and
d) To challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed, or amended.

Information

The use of data to extract meaning.

Information Disclosure

The exposure of information to individuals who normally would not have access to it.

Information Model

The characterization of the information that is associated with the use of a service. The scope of the information model includes the format of information that is exchanged, the structural relationships within the exchanged information, and the definition of terms used.

Information Privacy

Information privacy is the interest individuals have in controlling or at least significantly influencing the handling of data about themselves.

Information Quality

The accuracy and validity of the actual values of the data, data structure, and database or data repository design. The elements of information quality are accuracy, completeness, currency, reliability, and context/meaning.

Interaction

The activity involved in making use of a capability offered, usually across an ownership boundary, in order to achieve a particular desired real-world effect.

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.

Interface Description Requirements

Establishes common characteristics of service interface descriptions. These requirements address areas such as required interface contents, naming rules, documentation rules, and specification of a standard structure and format for descriptions.

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.

M

Memorandum of Understanding (MOU)

A legal document describing a bilateral agreement between parties. It expresses a convergence of will between the parties, indicating an intended common line of action, rather than a legal commitment.

Message

The entire "package" of information sent between service consumer and service (or vice versa), including any logical partitioning of the message into segments or sections.

Message Definition Mechanisms

Establishes a standard way of defining the structure and contents of a message; for example, GJXDM- or NIEM-conformant schema sets. Note that since a message includes the concept of an "attachment," the message definition mechanism must identify how different sections of a message (for example, the main section and any "attachment" sections) are separated and identified and how attachment sections are structured and formatted.

Message Exchange Patterns

Identifies common sequences of message transmission between service consumers and services. They provide a label to a series of message transmissions that have some logical interrelationship.

Message Validators

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

Metadata

Metadata is information (data) about a particular content (data). An item of metadata may describe an individual datum (content item) or a collection of data (content items). Metadata is used to facilitate the understanding, use, and management of data. The metadata required for this will vary with the type of data and context of use.

N

NIEM

National Information Exchange Model

Nonrepudiation

A technique used to ensure that someone performing an action on a computer cannot falsely deny that they performed that action. Nonrepudiation provides undeniable proof that a user took a specific action, such as transferring money, authorizing a purchase, or sending a message.

O

OECD

Organisation for Economic Co-operation and Development

Openness Principle

One of the eight Fair Information Principles developed by the Organisation for Economic Co-operation and Development. According to this principle, there should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal data and the main purposes of their use, as well as the identity and usual residence of the data controller.

OWL

Ontology Web Language

P

PAP

Policy Administration Point

PDP

Policy Decision Point

PEP

Policy Enforcement Point

Permissions

Authorization to perform operations associated with a specific shared resource, such as a file, directory, or printer. Permissions must be granted by the system administrator to individual user accounts or administrative groups.

Personal Data

Personal data refers to any personally identifiable information that relates to an identifiable individual or data subject. See also *Personally Identifiable Information*.

Personal Information

See *Personally Identifiable Information*.

Personally Identifiable Information (PII)

Personally identifiable information is one or more pieces of information that, when considered together or when considered in the context of how the information is presented or gathered, are sufficient to specify a unique individual.

The pieces of information can be:

- Personal characteristics such as height, weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious affiliation, place of birth, mother's maiden name, distinguishing features, and biometrics information, such as fingerprints, DNA, and retinal scans.
- A unique set of numbers or characters assigned to a specific individual, including name, address, phone number, social security number, e-mail address, driver's license number, financial account or credit card number and associated PIN number, Integrated Automated Fingerprint Identification System (IAFIS) identifier, or booking or detention system number.
- Descriptions of event(s) or points in time (for example, information in documents such as police reports, arrest reports, and medical records).
- Descriptions of location(s) or place(s), including geographic information systems locations and electronic bracelet monitoring information.

Privacy

The term *privacy* refers to individuals' interests in preventing the inappropriate collection, use, and release of personally identifiable information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data.

Privacy Impact Assessment (PIA)

An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Privacy Policy

A privacy policy is a written, published statement that articulates the policy position of an organization on how it handles the personally identifiable information that it gathers and uses in the normal course of business. The policy should include information relating to the processes of information collection, analysis, maintenance, dissemination, and access. The purpose of the privacy policy is to articulate that the agency will adhere to those legal requirements and agency policy determinations that enable gathering and sharing of information to occur in a manner that protects personal privacy interests. A well-developed and implemented privacy policy uses justice entity resources wisely and effectively; protects the agency, the individual, and the public; and promotes public trust.

Privacy Protection

A process of finding appropriate balances between privacy and multiple competing interests, such as justice information sharing.

Provider System

The information system that offers the use of capabilities by means of a service.

Provisioning Models

The responsibility or models for making a service available to customers in a manner consistent with formal (or occasionally informal) customer expectations.

Purpose Specification Principle

One of the eight Fair Information Principles developed by the Organisation for Economic Co-operation and Development. According to this principle, the purposes for which personal data are collected should be specified no later than at the time of collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

R

RDF

Resource Description Framework

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.

Record

Any item, collection, or grouping of information that includes personally identifiable information and is maintained, collected, used, or disseminated by or for the collecting agency or organization.

Reference Architecture

A reference architecture is an architectural design pattern that indicates how an abstract set of mechanisms and relationships realizes a predetermined set of requirements.

Reference Model

A reference model is an abstract framework for understanding significant relationships among the entities of some environment that enables the development of specific reference or concrete architectures using consistent standards or specifications supporting that environment. A reference model consists of a minimal set of unifying concepts, axioms, and relationships within a particular problem domain and is independent of specific standards, technologies, implementations, or other concrete details.

Repository

Stores models and interface descriptions in a central location that is accessible to appropriate stakeholders. A repository will permit searching for models and interface descriptions based on a range of identifying criteria. A repository will also map logical service identifiers with physical addresses.

Role-Based Authorization

A type of authorization that uses roles to determine access rights and privileges. A role is a symbolic category of users that share the same security privilege.

S

Secure Sockets Layer (SSL)

A protocol that provides secure data communication through data encryption. This protocol enables authentication, integrity, and data privacy over networks through a combination of digital certificates, public-key cryptography, and bulk data encryption. This protocol does not provide authorization or nonrepudiation.

Security

Security refers to the range of administrative, technical, and physical mechanisms that aim to preserve privacy and confidentiality by restricting information access to authorized users for authorized purposes. Computer and communications security efforts also have the goal of ensuring the accuracy and timely availability of data for the legitimate user set, as well as promoting failure resistance in the electronic systems overall.

Security Policy

A security policy is different from a privacy policy. A security policy alone may not adequately address the protection of personally identifiable information or the requirements of a privacy policy in their entirety. A security policy addresses information classification, protection, and periodic review to ensure that information is being stewarded in accordance with an organization's privacy policy. See *Privacy Policy*.

Security Safeguards Principle

One of the eight Fair Information Principles developed by the Organisation for Economic Co-operation and Development. According to this principle, personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data.

Service Agreement

A document that establishes policies and contractual elements for a given interaction or set of interactions (that is, for one or more services).

Service Consumer

An entity that seeks to satisfy a particular need through the use of capabilities offered by means of a service.

Service Contract

An agreement by two or more parties regarding the conditions of use of a service.

Service Design Principles

The documentation to provide consistent guidance regarding the overall partitioning of capabilities into services and the relationships between services.

Service Interaction Profiles

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 Global JRA 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 Interaction Requirements

Common rules of service interaction. Typically, these requirements are nonfunctional in nature, in that they are not directly related to the capability used by the service consumer, nor are they related to the real-world effect resulting from use of that capability. Rather, the requirements enforce (or support the enforcement of) policies or contracts or otherwise protect the interests of particular business partners or the business organization overall.

Service Interfaces

The means by which the underlying capabilities of a service are accessed.

Service Model

Interaction depends on two things. First, the designers of potential consumers need to be able to find services and, once found, establish a physical interaction mechanism with them. Second, the designers of potential consumers need a description of the actions that can be performed on a service, as well as the structure and meaning of information exchanged during the interaction. These needs are addressed by the concept of a service's information model and behavioral model, collectively called service models in the Global JRA.

Service Modeling Guidelines

Document guidelines for services provided and consumed among partners. They provide guidance as well as compliance information regarding the modeling and description of services to promote consistency.

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.

Service Policies

A statement of obligations, constraints, or other conditions of use, deployment, or description of an owned entity as defined by any participant.

Service Providers

An entity (person or organization) that offers the use of capabilities by means of a service.

Services

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

SPARCLE

Server **P**rivacy **AR**rchitecture and **C**apabi**L**ity **E**nablement is a Privacy Policy Workbench project conducted by IBM.

T

Transformers

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

U

Use

With respect to personally identifiable information, the sharing, employment, application, utilization, examination, or analysis of such information within the agency or organization that maintains the designated record set.

Use Limitation Principle

One of the eight Fair Information Principles developed by the Organisation for Economic Co-operation and Development. According to this principle, personal data should not be disclosed, made available, or otherwise be used for purposes other than those specified in accordance with the Purpose Specification Principle, except with the consent of the data subject or by the authority of law. See *Purpose Specification Principle*.

V

Visibility

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

W

Willingness

A predisposition of service providers and consumers to interact.

Appendix G: References

Global Infrastructure/Standards Working Group (GISWG), *Global Justice Reference Architecture (JRA) Specification,* Version 1.4, Working Draft, February 14, 2007, http://it.ojp.gov/topic.jsp?topic_id=242

Global Infrastructure/Standards Working Group (GISWG) *Global Justice Reference Architecture (JRA) Web Services Service Interaction Profile,* Version 1.1, August 31, 2007, http://it.ojp.gov/globaljra

Global Intelligence Working Group (GIWG), *Fusion Center Guidelines, Developing and Sharing Information and Intelligence in a New Era; Guidelines for Establishing and Operating Fusion Centers at the Local, State, and Federal Levels; Law Enforcement Intelligence, Public Safety, and the Private Sector*, http://it.ojp.gov/topic.jsp?topic_id=209

Global Justice XML Data Model (GJXDM), http://it.ojp.gov/jxdm/

Global Privacy and Information Quality Working Group (GPIQWG), *Privacy Policy Development Guide and Implementation Templates*, http://it.ojp.gov/documents/Privacy_Guide_Final.pdf

Global Security Working Group (GSWG), *Applying Security Practices to Justice Information Sharing,* May 2007, http://it.ojp.gov/documents/asp/default.htm

Global Security Working Group (GSWG), Global Federated Identity and Privilege Management (GFIPM) Metadata Package, Version 0.3, Working Draft, September 23, 2006, http://it.ojp.gov/topic.jsp?topic_id=248

Information Sharing Environment Implementation Plan, November 2006, http://www.ise.gov/content/library.htm

Microsoft, *The Identity Metasystem: Towards a Privacy-Compliant Solution to the Challenges of Digital Identity*, October 2006

National Information Exchange Model (NIEM), http://www.niem.gov/library.php

National Institute of Standards and Technology, Special Publication 800-95, *Guide to Secure Web Services*, August 2007, http://csrc.nist.gov/publications/nistpubs/800-95/SP800-95.pdf

Oracle Identity Services Framework, Working Draft 02, November 24, 2006

SEARCH, the National Consortium for Justice Information and Statistics, JIEM Tool, http://www.search.org/programs/info/jiem.asp