Part III — Technical Architecture

Chapter 8 — Technology Standards

Introduction

This chapter presents the technology standards associated with target technologies that will support the goals of the Medicaid enterprises. The primary focus is to select those technologies that meet the Medicaid IT Architecture (MITA) needs and to identify holes and deficiencies that must be solved uniquely for MITA. These standards support the analysis and tradeoffs that must be done between risk and value. An important part of the MITA life cycle will be an annual analysis of the available technology standards and definition of those standards that MITA recommends.

This chapter answers the following questions:

- What are the MITA technology standards?
- What is the MITA Standards Reference Model?
- What is the MITA Technology Standards Reference Guide?

Purpose

The use of open standards supports the reuse of solutions and facilitates commercial off-the-shelf (COTS) integration. The use of standards also enables interoperability of Medicaid enterprises.

Scope

MITA technology standards are quite dynamic and require a periodic review of the available technologies and definition of those that MITA recommends. Technology standards are classified into three categories:

- *Ready* — technology that is ready to be used
- *Emerging* — technology that will fit the needs of MITA over the next year
- *Incubating* — technology that is on a watch list as being nearly ready

The emerging technologies and processes that have the most significant impact are those involved with creating and enabling the definition of a service-oriented architecture (SOA) and the creation of distributed components.

Many of the technologies recommended in the standards are mature but may be unfamiliar to the MITA community. The preference is for open standards that are supported by two or more vendors. Interoperability and data management features will be based on open standards and will leverage similar initiatives within other government agencies.

Critical technologies to watch over the next 18 months include the maturing security and privacy (S&P) technologies and the model-driven architecture and implementation technologies that will allow the system model, configuration management, and dynamic configuration control of services distributed to be fully implemented.

What Are the MITA Technology Standards?

MITA technology standards identify target technologies that will support MITA business goals. The primary focus is on selecting standard technologies that will meet MITA needs and identify holes and deficiencies, if any, that must be resolved uniquely for MITA. An annual analysis of the available technologies to define those that MITA recommends will be part of the MITA life cycle.

What Is the MITA Standards Reference Model?

The MITA Standards Reference Model (SRM) is a framework that identifies technical services for which MITA identifies standards. The MITA SRM is shown in **Figure 8-1**. The SRM consists of technical services/capabilities, which are shown as a series of horizontal layers and vertical slices that cut across the layers. The horizontal layers represent six separate areas of technology standards and evolving technology: user interface, message exchange, metadata repository, message transmission, data and information, and communication.

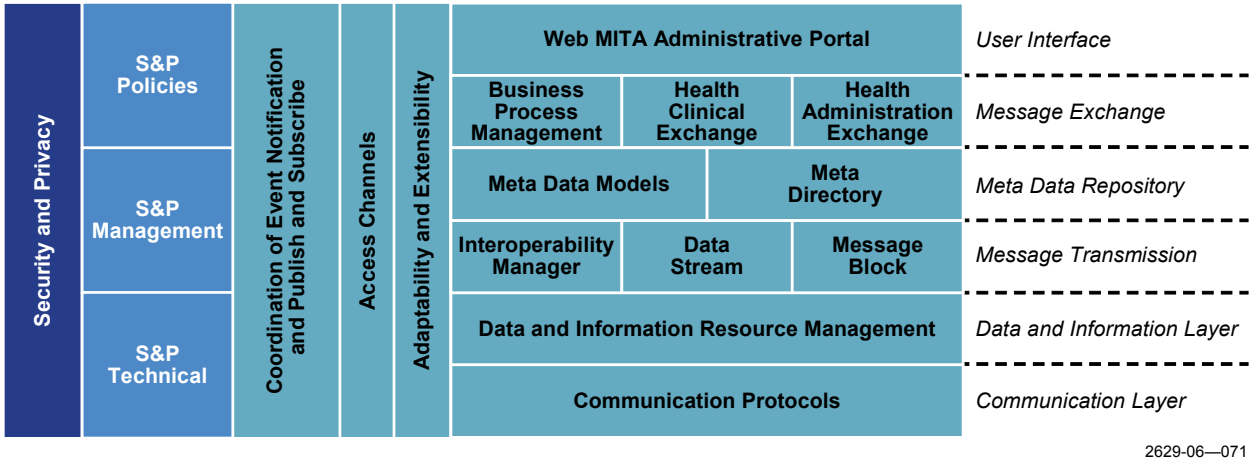

Figure 8-1. MITA Standards Reference Model

The four vertical slices of the SRM shown in Figure 8-1 are:

- S&P services, which include policy, management, and technical service elements
- Coordination of event notification and publish-and-subscribe
- Access channels

- Adaptability and extensibility services, which operate with each of the layers to design and manage changes in a consistent manner

The SRM provides the framework for categorizing the MITA-recommended technology standards. The SRM provides information about each standard that a State can use in its procurement specification to align itself with MITA standards and to use as an information resource. For example, it has included pointers into which standards committees are active and can be used in architecture efforts of the Department of Health and Human Services (DHHS) or States. MITA will refine its efforts based on feedback from States and the vendor community.

The selected standards were chosen for their strong focus on service integration and their capability to be used in architectures that cross interstate and intrastate boundaries. These criteria will encourage interfaces and data sharing standards that are consistent with the intent of the National Health Information Infrastructure (NHII) initiative.

The SRM provides an overview of the current taxonomy of standards and how they relate to different solution sets.

Key Elements of the Standards Reference Model

The six layers in the SRM are as follows:

- **User Interface.** Standards for user interaction with Medicaid systems that use a wide range of devices, including desktops, laptops, PDAs, mobile phones, and others.
- **Message Exchange.** Standards for message content exchanged between MITA applications, including messages exchanged between and within business processes, health clinical data, and health administration data.
- **Metadata Repository.** Standards for metadata interchange among data warehousing, business intelligence, and portal applications that provide a common basis for metamodels that bridge gaps between dissimilar metamodels. Two sets of standards are in this layer: metadata models and metadata directory. MITA will provide metadata management services to find, access, and create virtual queries that span organization boundaries and support translations from two aligned but different syntaxes, using metadata transformation tools.
- **Message Transmission.** Standards for end-to-end message routing based on logical need. These standards use communication layer protocols for message transport over communications links and networks. The Electronic Data Interchange (EDI) Gateway and the Enterprise Service Bus (ESB) will be primary elements within this level. One of the key purposes of following standards is to ensure that service-oriented message delivery with XML capabilities will be part of the external exchange between ESB and that translation is handled at the EDI Gateway by the transmitting organization.
- **Data and Information Resource Management Layer.** Standards through data management and services that can access structured data using the SQL, semistructured

data using XML-based queries (e.g., XQuery), and unstructured data using content management and search tools that understand HTML and the Dublin Core.

- **Communications Layer.** Standards for communications protocols used at the lowest four layers defined in the ISO Open Systems Interconnection Model (i.e., the physical, link, network, and transport layers).

In addition to the standards at the six layers described above, the reference model describes standards for four additional areas that span multiple SRM layers:

- **Security and Privacy.** S&P standards will provide a level of consistency focused on the tactical sharing of data.
- **Coordination of Event Notification and Publish-and-Subscribe.** These standards support information sharing and change management with process automation functions. They support an event-driven architecture and information exchange and service requests consistently within and across States.
- **Access Channels.** These standards enable transparent access among MITA applications and between users and MITA applications. A variety of devices (e.g., PDAs, wireless phones, and WiFi routers) can interface with MITA applications through special device managers.
- **Adaptability and Extensibility.** These standards reflect technical features and parameters that can be changed within each of the layers. Changes can be managed in an orderly way.

Applicable Standards

This section presents currently defined MITA standards for the services/capabilities described in previous sections. The standards will be updated and refined in MITA Framework 3.0.

User Interface Layer Standards

MITA Web Administrative Portal will focus on the tools needed to adapt and manage the shared services and tactical and strategic data access to provide tools but manage control within limits set by the governance process. MITA will base the portal on Web Services (WS) Remote Management Portlet standards. The operational and the administrative portals will both follow the same basic standards.

Message Exchange Layer Standards

Business Process Management Standards will be used within the process automation service, which will enable the addition of new business areas or provide the ability to compose processes and link to COTS capabilities. A Business Process Management Notation (BPMN)-defined model will be directed to a Web Services-Business Process Execution Language (WS-BPEL) with human interaction extension to address workflow and business process automation issues.

Clinical Health Exchange will involve HL7 Exchange, which handles classes of event-based HL7 messages.

Health Administration Exchange, including Health Insurance Portability and Accountability Act of 1996 (HIPAA) and related privacy services, will be handled as discussed in the HIPAA Exchange and Related Attachments.

Metadata Repository Layer Standards

Federated Data Management Engine is a registry or repository that can create virtual models and can map between data sets that States, providers, or Federal agencies can own but agree to share based on an access-control agreement. The "federated" part is a small central core of the virtual model or virtual schema that links to the related data elements. It can be used for short-term, focused problems as a transition strategy to the more tactical or strategic shared data or enable drill down to data that comes from a subject-specific data mart. An XML-SQL interface will provide virtual data access.

Metadata. The recommended metadata standard for MITA is MetaObject Facility (MOF) Version 2.0 and WS Metadata Exchange capability, coupled with XML Schemas. Specific metadata elements from other standards will be integrated. Each State will have extensions and overrides to the base metadata.

Message Transmission Layer Standards

Interoperability Manager will provide the management of new interfaces as new NHIIs are created. Its focus will be on creating business agreements between organizations at the policy level and establishing specific information exchanges and specific, permissible, fine-grained queries. This function will manage the business interface agreements (e.g., formats, security, and policy elements), monitor for compliance, and provide failover and recovery and flow management. It will be based on Messaging Electronic Business XML (ebXML) and emerging business-centric interface management methodology. Channels and WS endpoints based on WS Addressing and WS Choreography Description Language will be part of the information used by the interoperability manager. MITA will provide WS Reliable Messaging and other resilience standards for guaranteed delivery of messages for critical business exchanges.

Data Stream reflects the use of XML-based protocol standards that cover message headers, enable the routing of messages to the right location based on logical need, and map between logical and physical need based on the type of message received. Smart telecommunication switches and topic-based virtual communication channels are a key element of the interface-integration-interoperability layer. Event-based detection and filtering, such as with WS Eventing and WS Notification (WSN), will be considered here.

Simple Object Access Protocol (SOAP) Message Exchange (MSX) is a set of message exchange enablers (SOAP 1.2 is operational and SOAP 2.0 is emerging). The MITA team will consider new performance-enhanced forms of SOAP MSX based on brief treatment outcomes measure (BTOM) and other performance-based standards enhancements. Messages will be signed and selectively encrypted. All messages will be labeled to designate specifically the owner and the S&P policies it must follow.

Security and Privacy Standards

S&P standards will address policies, management procedures, and technical services that cover technical functions (e.g., authentication, authorization, and auditing) and ensure that security policies are enforced between MITA services.

Coordination of Event Notification and Publish-and-Subscribe Standards

These standards will leverage the Organization for the Advancement of Structured Information Standards (OASIS) WSN family of specifications that define standard interoperable protocols through which WS can be disseminated as events. The WSN family includes the following:

- **WS Base Notification** specification defines the WS interfaces for notification producers and notification consumers. It includes standard message exchanges that service providers can implement and the operational requirements expected of them. This is the base document on which the other WSN specification documents depend.
- **WS Topics** specification defines a mechanism to organize and categorize items of interest for subscription (known as *topics)*. These are used in conjunction with the notification mechanism defined in WS Base Notification. WS Topics specifies an XML model for describing metadata associated with topics and defines some topic expression dialects that can be used to refer to them.
- **WS Brokered Notification** specification defines the WS interfaces for notification brokers. A notification broker is an intermediary that, among other things, allows publication of messages from entities that are not themselves service providers (e.g., the service gateways and information hub). It includes standard message exchanges that notification broker service providers can implement, along with operational requirements expected of service providers and requestors that participate in brokered notifications.
- **WSN Notification Policy** specification defines policy statements that can be used in conjunction with other specifications in the family to request particular qualities of service or other activities.

The ESB will provide the service-oriented infrastructure to address request/response style messages and event-based message exchanges that follow these standards.

Access Channels Standards

PDAs and portals will be two major types of access mechanisms. The PDAs will use a Web browser that is compliant with XHTML and CSS2. The Infrared Data Association will be used, along with TCP/IP and Point-to-Point Tunneling Protocol (PPTP), Internet protocol security (IPSEC), and SecureShell. Other access channels will be defined as needs are identified.

Adaptability and Extensibility Standards

Three levels of standards have been identified:

- Standards that involve defining user needs and the variety of elements that the users can access. These include the services the user needs to perform a task and the related message exchanges, metadata that the user can access, message transmissions and their permitted message-exchange patterns, and data and information components and resources that the user can access. Only research and proprietary activities are in these service management models. WS Coordination and WS Management protocols will be used in a selective manner.
- Standards such as the WS Distributed Management and changes within enterprise management to address service orientation. The managed service environment must respond to changes in user needs and preferences; support the evolution of services in phased sets of service collations or epochs; and react to the addition, deletion, or temporary changes of resources.
- Resource management is being addressed in standards in the WS Resource Framework that are now being integrated with the experience from the grid computing experience from the science and research community. The standards define service groups and their directory, a standard method of defining the properties of WS resources, their lifetime management, and their ability to handle faults in a consistent manner. The WSN defined under the Coordination of Event Notification and Publish-and-Subscribe Standards will be used to identify and broker changes to appropriate service groups.

Service Delivery and Service Support

Similar IT Service Management capabilities will complement the MITA SRM to address the service delivery and service support functions. IT services must be addressed from both the service provider and service client perspective. Many Medicaid providers will work in many States and will expect similar services and interactions. Beneficiaries who move from State to State or into different systems within the same State will expect the same service. IT Service Management quality and service delivery and support service requirements can be defined based on emerging standards such as eSourcing Capabilities Model for Service Provider (eSCM-SP) (April 2004), with its 84 Practices, the eSourcing Capability Model for Client Organization (eSCM-CL) (February 2006), with its 98 practices, and other elements such as those in the IT Information Library of best practices for IT Service Management.

The Services Support Center (SSC) must address the following areas and support the people that have the relevant knowledge and execution skills. Service delivery covers the processes required for the planning and delivery of quality IT services and looks at the longer term processes associated with improving the quality of delivered IT services. Service delivery includes the following areas:

- **Service Level Management (SLM)** negotiates, documents, agrees to, and reviews business service requirements and targets within service level requirements and service

level agreements. These pertain to the measurement, reporting, and reviewing of the quality of services IT delivers to the business. The SLM process also negotiates and agrees to support targets contained in operational level agreements with the support team.

- **Capacity Management** processes ensure that adequate capacity is available at all times to meet the requirements of the business by balancing business demand with IT supply. Capacity plan is closely connected to the business strategy and includes performance management, workload management, demand management, and application sizing and modeling.
- **IT Service Continuity Management** produces recovery plans designed to ensure that IT services will continue on an agreed level and within an agreed schedule following any major incident that disrupts or might disrupt service. It is a component of a business continuity planning process.
- **Financial Management for IT Services** provides the basis for running IT as a business within a business and for developing a *cost-conscious* and *cost-effective* organization.
- **Availability Management** is responsible for ensuring that services meet or exceed their availability targets and are proactively improved on an ongoing basis.

Service support describes the processes associated with providing IT services, especially in the following areas:

- **Configuration Management** is the foundation for successful IT Service Management and underpins every other process.
- **Problem Management** minimizes adverse impacts from incidents and problems in the business, assists incident management, and seeks to prevent incidents and problems.
- **Change Management** supports the efficient and effective management of changes through the complete life cycle. It focuses on the forward scheduling of changes throughout the organization based on business impact and urgency.
- **Service Desk** provides a single, central point of contact for all IT users in an organization and handles all incidents, queries, and requests. It provides an interface for all other service-support processes.
- **Release Management** takes a holistic view of changes to IT services, considering all technical and nontechnical aspects of release planning and follow through.
- **Incident Management** manages all incidents, from detection and recording through resolution and closure. Incident management seeks to restore normal services as soon as possible and with minimal disruption to the business.

Technology Readiness and Maturity

As shown in **Figure 8-2,** technology readiness and the MITA Maturity Model (MMM) provide an invaluable resource for States to use in planning and coordinating their technology acquisition to foster innovations during a long procurement cycle. Technology readiness operates in tandem with the annual technology review.

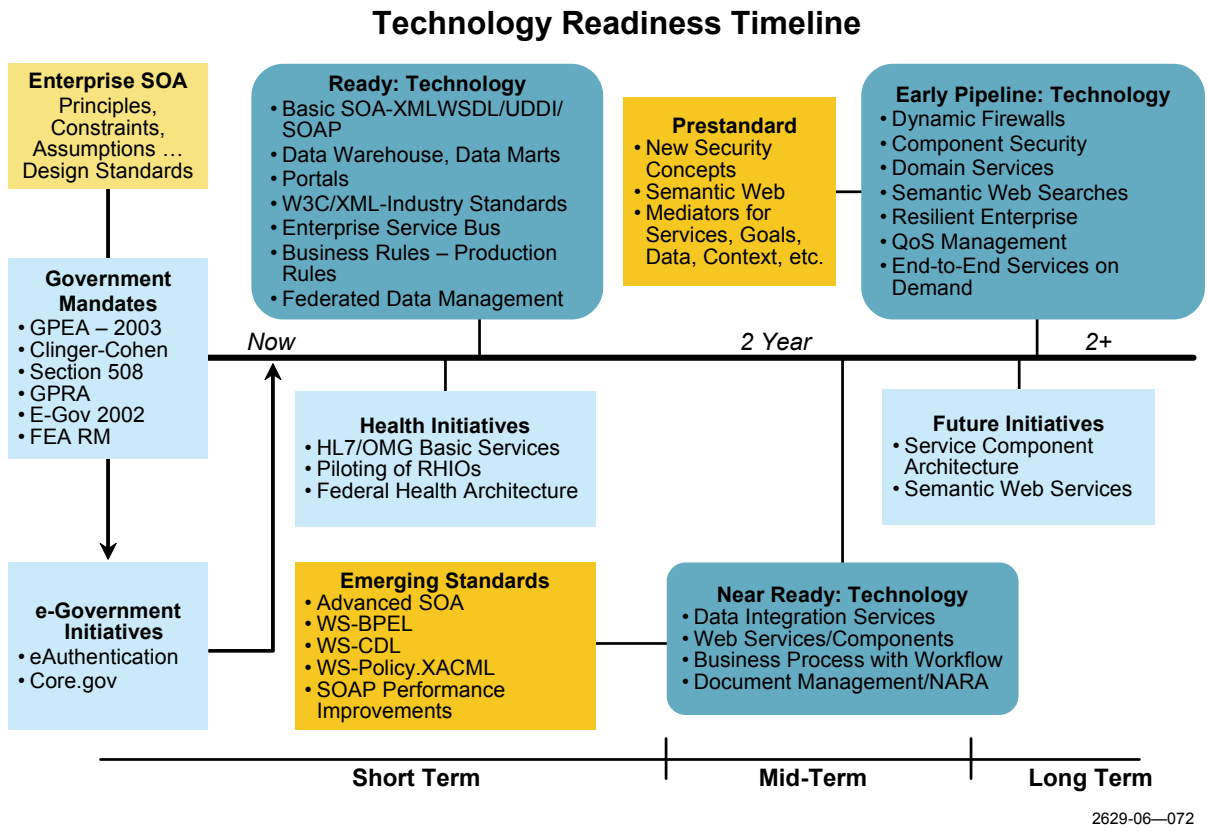

Figure 8-2. Technology Readiness and the MITA Maturity Model

A principal purpose of technology management is to understand the maturity of a State's current technology and the business value of new and emerging technologies to improve benefits. A systematic technology management process will prevent "vendor push" and identify gaps and needs. Technology drivers (e.g., government mandates and initiatives) can follow overall guiding principles and assumptions and identify mature technologies or emerging and new technologies. Figure 8-2 represents a snapshot of MITA-related technologies. Annual or semiannual readiness roadmaps can be created and discussed to achieve business–technology alignment.

Key Elements of the Technology Readiness and Maturity

The SRM and related analyses identify key drivers at the top, including government mandates and drivers specific to MITA (e.g., the Federal health initiatives, Regional Health Information

Organizations, National Health Information Network, and Health Level 7 [HL7]/Object Management Group [OMG] service specification) or other government initiatives that can be used as MITA components (e.g., Federal e-Government initiatives such as e-Authentication and other elements that can be found in www.core.gov). Many open-source and industry initiatives can also be included in the timeline along with initiatives in specific States or region.

The essential purpose of the SRM is to identify technologies that are *ready* (i.e., ready for use), *emerging* (i.e., will fit MITA's needs over the next year), and *incubating* (i.e., on a watch list and is nearly ready). Classifying technologies this way involves judgment calls that will be discussed within the appropriate portfolio area. The emerging technologies and processes that will have the most significant impact are those involved with creating and enabling the definition of a SOA and the creation of distributed components. Many technologies recommended in the SRM are mature but may be unfamiliar to the MITA community. The preference is for open standards that have two or more vendors supporting them. Interoperability and data management features will be based on open standards and will leverage similar initiatives within other government agencies. Critical technologies to watch over the next 18 months include maturing S&P technologies and model-driven architecture and implementation technologies that will allow the full implementation of the system model, configuration management, and dynamic configuration control of services distributed.

What Is the MITA Technology Standards Reference Guide?

Overview

The MITA Technology Standards Reference Guide (TSRG) is a collection of standards applicable to the administration and operation of a Medicaid enterprise. Each standard is defined by the following attributes:

- Title
- Category
- Objective
- Source (Standards Body)
- Type
- Versions and Status
- Applicability
- References
- Relationships to Other Standards
- Key Terms

An example of the template used to capture this information is shown in **Table 8-1**.

Table 8-1. Standards Definition Template

Standards Definition Template	
Title	The standard's title should be provided in the following format: Spelled-out standard (ACRONYM) Example: ■ Web Apps Compound Document
Category	The appropriate solution sets (this links to a portfolio area)
Objective	The purpose of the standard (i.e., why do we need to have this standard?)
Source: (Standards Body)	The name of the standards body or organization responsible for the standard Example: ■ www.w3c.org
Type	The people who care about and use the standard or how broadly it is applied (*Basic* means the standard applies to just about everybody, while *Advanced* applies to people with more complex needs) ■ <Basic>
Versions and Status	The recommended version number and any available information about upcoming versions and enhancements Example: ■ Version
Applicability	Summary of the content/focus of the standard
References	Links to Web sites where the latest information can be found
Relationships to Other Standards	Other standards that rely on or impact this standard
Key Terms	Terms and definitions that are critical to understanding the standard

The standards identified in the associated standards templates will relate to the key design aspects and concepts that are being further defined in the MITA Framework.

MITA Technology Standards Reference Guide

This section provides the technology standards used by the MITA Technical Architecture. It provides guidance for those technology standards most important for developing MITA systems.

> This version of the MITA Technology Standards Reference Guide contains placeholders for every identified standard, but only a portion of those standards have the corresponding template.

The organization of the TSRG reflects the need for periodic updates. Architecture, analysis, and design standards are organized around MITA technical areas with an additional section devoted to standards about architecture. Additionally, there is a "medical information" group of standards and a group for any Medicaid-specific standards. As MITA identifies relevant standards, they will be added or updated in the TSRG. These standards will be linked to the MITA Logical Architecture. The TSRG will reside in the MITA repository once the repository is operational.

Standards are at varying levels of maturity. Some standards are ready for use today, some are emerging, and others are in a stage referred to as "incubating." The term *incubating* describes a standard that is developing convergence and may require 3 to 5 years before it is finalized and adopted.

Architecture, Analysis, and Design Standards

1. Object Management Group
   a. Model-Driven Architecture
      (1) Unified Modeling Language (UML) 2.0
      (2) MetaObject Facility
   b. BPMN, Business Process Definition Metamodel (BPDM), and the many other business models
   c. UML Enterprise Distributed Object Computing (EDOC), SOA, and other profiles of importance
   d. UML Service-Oriented Architecture Profile
2. World Wide Web Consortium (W3C)
   a. Web Ontology Language (OWL-S)
   b. Web Service Definition Language (WSDL)
3. OASIS
   a. Universal Business Language
   b. WS-Composite Application Models
   c. Web Application Compound Document
4. Research and Open-Source Initiatives
   a. Web Services Modeling Framework
   b. Enterprise Modeling and updating of the Reference Model for Open System Operations
   c. Open standards such as Eclipse

Service Interoperability

1. Basic Web Services Profile
   a. XML
   b. SOAP
   c. Universal Description, Discovery, and Integration (UDDI)
   d. HTTP/HTTPS

e. WSDL 1.0
f. Open issues and interoperability workshops and tests

2. Advanced Web Service Profile
   a. WSDL 2.0
   b. Messaging with ebXML
   c. WS-Policy (**Table 8-2**)
   d. WS-Agreement (**Table 8-3**)
   e. WS-Context
   f. WS-Addressing (**Table 8-4**)
   g. WS-Reliability (**Table 8-5**)
   h. SOAP with attachments-MTOM
   i. DARPA Agent Markup Language (DAML-S)
   j. OWL-S
3. Business Line Agreements
   a. ebXML-trading partner agreements and ebXML SOA
   b. Service Level Arrangement Language (SLAlang)
   c. UBL-Resource Event Action Model
4. Management and Control
   a. Web Service Distribution Management (WSDM)
   b. Web Services Reliable Messaging (WSRM) (**Table 8-6**)
   c. IT Infrastructure Library (ITIL) — IT Service Management Capabilities Level
      (1) This is an IT management standardization effort to understand and compare the IT resource utilization and addressing in order to improve the effectiveness and efficiency of the infrastructure used.
   d. Distributed Management Task Force (DMTF) Common Information Model (CIM) and other standards
      (1) DMTF has been working on infrastructure management and has developed a series of standards that are gaining acceptance in the system management industry segment (www.dmtf.org).
      (2) CIM is an object-oriented model that describes the conceptual framework for describing management data.
      (3) CIM messages can now be exchanged in XML format and over HTTP.

(4) CIM messages are well-defined request or response data packets used to exchange information between CIM products. There are two types of CIM messages: CIM Operation Messages and CIM Export Messages.

(a) A CIM Operation Message is a CIM message used to invoke an operation on the target namespace.

(b) A CIM Export Message is a CIM message used to communicate information about a CIM namespace or element that is foreign to the target. A CIM Export Message is informational only and does not define an operation on the target CIM namespace or even imply the existence of a target namespace.

Table 8-2. Web Services Policy Framework

Standards Definition Template	
Title	Web Services Policy Framework (WS-Policy)
Category	Service Interoperability
Objective	Provides a mechanism for addressing endpoints, shipping those addresses in messages, and addressing those messages to those endpoints.
Source: (Standards Body)	W3C
Type	The WS-Policy provides a general-purpose model and corresponding syntax to describe and communicate the policies of a Web service. WS-Policy defines a base set of constructs that can be used and extended by other Web services specifications to describe a broad range of service requirements, preferences, and capabilities.
Versions and Status	Currently in initial submission stage by a consortium of companies (September 2004) and will undergo a year-long public review (December 2005). A candidate recommendation may come out in this area.
Applicability	WS-Policy provides a flexible and extensible grammar for expressing the capabilities, requirements, and general characteristics of entities in an XML Web services-based system. WS-Policy defines a framework and a model for the expression of these properties as policies. Policy expressions allow for simple declarative assertions as well as more sophisticated conditional assertions. WS-Policy defines a *policy* to be a collection of one or more policy assertions. Some assertions specify traditional requirements and capabilities that will ultimately manifest on the wire (e.g., authentication scheme and transport protocol selection). Some assertions specify requirements and capabilities that have no wire manifestation but are critical to proper service selection and usage (e.g., privacy policy and QoS characteristics). WS-Policy provides a single policy grammar to allow both kinds of assertions to be reasoned about in a consistent manner.

Standards Definition Template	
Applicability (Cont'd)	WS-Policy stops short of specifying how policies are discovered or attached to a Web service. Other specifications are free to define technology-specific mechanisms for associating policy with various entities and resources. Subsequent specifications will provide profiles on WS-Policy usage within other common Web services technologies.
References	www.w3c.org
Relationships to Other Standards	This standard must link tightly with the WSDL and SOAP standards and must provide a coherent foundation for any reliable messaging and resource-management tasks. End-to-end addressing is a critical element in defining a Web services-based SOA. It must work with the WS-Security family of standards.
Relationship to Security and Privacy Standards and Attack Patterns	WS-Policy must be aligned with security and privacy policies. There currently is a gap in this area that will have to be addressed.
Key Terms	

Table 8-3. WS-Agreement

Standards Definition Template	
Title	WS-Agreement
Category	Service Definitions, Business Process, and Meta Model Management
Objective	The agreements among service providers that are working together are described with a set of agreement behaviors among the delivered services with respect to the agreement initiator and service consumers. These agreements establish an ongoing relationship within a community creating what is often called a "virtual community" or in the Federal government would be called a "line of business." Each agreement represents a stable, named representation of the promised service behavior where many volatile details are abstracted to simply the presentation of predictable or expected behavior in terms of agreement negotiation.
Source: (Standards Body)	WS-I and the Open Grid Services Infrastructure have worked together to form an initial draft submitted to OASIS standard.
Type	Advanced
Versions and Status	Draft Version 3/10/2004

Standards Definition Template	
Applicability	Support between Federal and State organizations where services and information must be integrated for a special study or an ongoing business transaction and analysis relation need to have agreements. Those agreements are often informal or in written forms (e.g., a memorandum of understanding [MOU]), but as the systems become more sophisticated and key concerns arise (e.g., security and privacy protection and how the information can be used and shared) those agreements must be made more formal. Eventually, the vision of this standard is to have discovery and negotiation done through automated support called "software agents." Within the science community, a set of "agreements" have been made to exchange and share data with a grid services framework. These grid services agreements are being integrated with the WS-Agreement approaches, along with service management mechanism, to ensure that the agreement is being satisfied and violations are being flagged. Key concepts in the agreement activities include the following: **Agreement creation** includes defining the port types and negotiation of the types of agreements: **Negotiability Constraints in WS-Agreement (Version 0.1 Jan 2004)** enables the choice of one of more terms during negotiation and the customization of individual terms based on extension terms. Discovery of agreement templates with policies and the tailoring of those templates to reflect the organization's needs is still being refined and may have to be defined for the specific type of service and information integration patterns. Agreement templates will allow for adaptation and tailoring for each line of business and service-topic need. ■ **Agreement Lifetime** defines the state of agreement and those activities that must be done, may be done, and cannot be done and includes recommendations of what should be done. ■ The agreement can include specific guarantees of service quality from the service initiator (Guarantee Terms in WS-Agreement). These include the following: – **Qualifying conditions** are conditions under which a specific guarantee is to be observed (e.g., date and time of service delivery). – **Service Level Objectives** is expressed as conditions over the attributes of the service that must be met. – **Business Value** indicates the importance of the associated services with meeting this guarantee. This can be defined in relative and absolute terms so that tradeoffs can be made on level of importance and recovery strategies can be done. ■ **Agreement Termination** defines how the initiator should utilize services that cancel all terms of the commitments. **Audit and Finalization** describes the observed service behaviors that are reported.
References	
Relationships to Other Standards	
Key Terms	

Table 8-4. WS-Addressing

Standards Definition Template	
Title	WS-Addressing
Category	Service Interoperability
Objective	Provides a mechanism for addressing endpoints, shipping those addresses in messages, and addressing those messages to those endpoints.
Source: (Standards Body)	W3C
Type	This is a key element in the definition of a complete end-to-end process flow. All the middleware and service-delivery companies are interested in this standard because it is one of the key elements for adding more resource definition information to the uniform resource identifier (URI) points. It is currently divided into three major pieces, but more may be added: ■ Core ■ SOAP binding ■ WSDL binding with WSDL 1.1
Versions and Status	This is currently in draft stage but is building upon earlier work on the WS-Message Delivery effort. It has been in public review and issue resolution from February 2004 to February 2005.
Applicability	■ It provides a transport-neutral method to address WS and messages. ■ WS-Addressing Core defines a set of abstract properties and an XML Information Set (XML Infoset) representation to identify WS endpoints and to secure end-to-end identification of endpoints in messages. This specification enables messaging systems to support message transmission through networks that include processing nodes such as endpoint managers, firewalls, and gateways in a transport-neutral manner. ■ WS-Addressing SOAP Binding defines the binding of the abstract properties defined in WS-Addressing Core to SOAP messages. ■ Addressing can be used within SOAP messages to define various properties, including action, source, destination, message ID, etc. ■ Endpoints are not constrained but can be constructed, partitioned, named, and addressed in an arbitrary fashion. ■ Endpoints are defined by endpoint references and include both addresses and subaddresses. ■ Endpoint properties are a very important construct to be done in a consistent manner and endpoint references appear in 6 different protocols. ■ Consistent use of this standard will be critical to end-to-end interoperability. Currently WSDL 1.1 has limited extensibility and the service element is not consistent with the concepts of dynamic messaging and taking actions along the path from end to end based on the endpoint references. ■ Fault management is very difficult. Where do you send an error notification? This question is will be resolved by aligning WS-Addressing with WSDL 2.0 and SOAP, and it will allow the additional resource management standards to be coherently defined.
References	www.w3c.org

Standards Definition Template	
Relationships to Other Standards	This standard must link tightly with the WSDL and SOAP standards and must provide a coherent foundation for any reliable messaging and resource-management tasks. End-to-end addressing is a critical element in defining a WS based SOA. ■ It must work with the WS-Security family of standards.
Relationship to Security and Privacy Standards and Attack Patterns	The following list summarizes common classes of attacks that apply to this protocol and identifies the mechanism to prevent/mitigate the attacks: ■ Message alteration is prevented by including signatures of the message information using WS-Security. ■ Message disclosure is avoided by encrypting sensitive data using WS-Security. ■ Address spoofing is prevented by ensuring that all addresses are signed by a party authorized to speak on behalf of the address. ■ Key integrity is maintained by using the strongest algorithms possible (by comparing secured policies). ■ Authentication may be established using the mechanisms described in WS-Security. ■ Accountability is a function of the type and strength of the key and algorithms being used. In many cases, a strong symmetric key provides sufficient accountability. However, in some environments, strong public-key infrastructure (PKI) signatures are required. ■ Availability attacks of many varieties affect all reliable messaging services. Replay detection is a common attack, and it is recommended that this be addressed by the mechanisms described in WS-Security and/or caching of message identifiers. Other attacks (e.g., network-level denial-of-service attacks) are harder to avoid and are outside the scope of this specification. However, care should be taken to ensure that minimal state is saved prior to any authenticating sequences. ■ Replay of messages may happen for a variety of reasons. To detect and eliminate this attack, mechanisms should be used to identify replayed messages (such as the timestamp/nonce outlined in WS-Security). Alternatively (and optionally), other technologies can be used to prevent replay of application messages (e.g., sequencing).
Key Terms	A *WS endpoint* is a (referenceable) entity, processor, or resource to which WS messages can be targeted. Endpoint references convey the information needed to identify/reference a WS endpoint and may be used in several different ways, including the following: ■ To convey the information needed to access a WS endpoint ■ To provide addresses for individual messages sent to and from WS *Message addressing* properties enable the identification and location of the endpoints involved in an interaction. The basic interaction pattern from which all others are composed is "one way." In this pattern, a source sends a message to a destination without any further definition of the interaction. *Request Reply* is a common interaction pattern that consists of an initial message sent by a source endpoint (the request) and a subsequent message sent from the destination of the request back to the source (the reply). A reply can be an application message, a fault, or any other message.

Table 8-5. WS-Reliability

Standards Definition Template	
Title	WS-Reliability
Category	Reliability
Objective	
Source: (Standards Body)	WS-I and OASIS-Open
Type	Advanced
Versions and Status	Draft Document January 8, 2003
Applicability	WS-Reliability is a SOAP-based protocol for exchanging SOAP messages with guaranteed delivery, no duplicates, and guaranteed message ordering. WS-Reliability is defined as SOAP message header extensions and is independent of the underlying protocol. It includes a binding to HTTP. The focus is on business-to-business (B2B) reliable message delivery. The specification borrows from previous work in messaging (e.g., ebXML) and transport and can be applied to WS services.
References	
Relationships to Other Standards	■ W3C SOAP 1.1/1.2 ■ OASIS ebXML Message Service Specification 2.0 ■ OASIS WS-Security
Key Terms	■ Asynchronous messaging at the application level ■ Guaranteed delivery ■ Duplicate elimination ■ Message ordering ■ It does not handle application-level synchronous messaging

Table 8-6. E Modeling Stateful Resources with Web Services

Standards Definition Template	
Title	WS-Resources
Category	Resources
Objective	WS-Resources involves modeling stateful resources with WS. It provides a common way of declaring and implementing Web services and tying them to stateful components. It provides the approach to define implied resource pattern usage and an approach to making WS-Resources accessible through a service interface as specified within the WS-Resource lifetime.
Source: (Standards Body)	
Type	Advanced
Versions and Status	
Applicability	
References	

Standards Definition Template	
Relationships to Other Standards	
Key Terms	

Security and Privacy

1. The Federal Enterprise Architecture (FEA) Security and Privacy Profile (SPP) and National Institute of Standards and Technology (NIST) Initiatives
   - A new document is being completed and plans involve adding services document and mapping to the standards.
   - MITA will be involved and tracking the FEA SPP and the changes in the NIST specifications as indicated by the eGov2002 Act.
2. HIPAA Security and Privacy Rule
   - Gather experience and understand if there are plans to update and refine.
3. XML Encryption
4. WS-Security — WS-I Security Profile (**Table 8-7**)
5. Liberty Alliance — Federated Approach (**Table 8-8**)
6. Security Assertion Markup Language (SAML) (**Table 8-9** and **Table 8-10**)
7. Platform for Privacy Preference Project (P3P) — W3C
8. Extensible Application Markup Language (XAML)
9. Enterprise Privacy Authorization Language (EPAL) — W3C (**Table 8-11**)
10. WS-Trust Model (**Table 8-12**)
11. eAuthentication and use of services — OMG initiative
    - The government is considering extending and adding additional security and privacy services. OMG has an additional security team. Track the FEA SPP and its future impact on MITA.
12. PKI (**Table 8-13**)
13. Health Security (**Table 8-14**)
    - It is important to gather information on the HIPAA experience and understand the HER/HL7 Security considerations.
14. UMLsec and Security Engineering Profiles
    - Efforts to create new security stereotypes to integrate them with the UML 2.0 activity diagrams along with other formal Message Sequence Chart extensions will be reviewed.

15. Security and Privacy Data Content Labeling and XML Access Authorization
    - Oracle Labeling has strong appeal, and there is extensive background information on distributed labeling (e.g., the work at Cornell by Andrew Meyers, et al). This will be needed for cross-line of business security and privacy control.
16. Data Management and Data Sharing
    a. Data Definition Languages
        (1) Structured–Relational Models — SQL (**Table 8-15**)
        (2) XML (**Table 8-16** through **Table 8-19**)
        (3) XML Schema (**Table 8-20**)
        (4) Name-space definitions — XML-Name-spaces
        (5) Directory of data elements
        (6) SQL/XML (**Table 8-21**)
        (7) XSL Transformations (XSLT) (**Table 8-22**)
        (8) XMLSQL
        (9) XQuery (**Table 8-23** and **Table 8-24**)
    b. Metadata and Registry Standards
        (1) ISO-11179
        (2) MOF
        (3) Metadata Exchange
        (4) Metadata Access Services
        (5) Grid Data Services (**Table 8-25**)
    c. Data in Motion — Data Services for Exchange

        Emphasis will be on using the ideas and concepts being worked out on cross-governmental line-of-business interoperability within the FEA Data and Information Reference Models and its use of OASIS, W3C, and OMG standards and tying to Web Service Interoperability and Liberty Alliance.
        (1) Cross-Enterprise
        (2) Inter-Enterprise
        (3) Data Storage Management (**Table 8-26**)
    d. Document and Forms Management Archive and Digital Libraries
        (1) Dublin Core

e. Healthcare Data Standards and Services for Data Access

There are many sources of information on standards efforts but the Robin Covers pages have recently been updated and have many fine sources of information can be found at — http://xml.coverpages.org/healthcare.html

(1) Relationship to Consumer Health Informatics (CHI) Initiatives and NHII/FHA
   (a) Collaborate with the Veterans Health Administration (VHA) on Common Data Services
   (b) FEA DRM
   (c) Line of Business Data Services Standards.

(2) Services for Data Access Perspective
   (a) Common Health Access and Context-Sensitive Access
   (b) European Committee for Standardization Technical Committee 251 (CEN/TC 251)
   (c) Service Definition Process

(3) HL7/HER and the move to services with collaboration with the OMG Healthcare Domain Task Force (**Table 8-27**)

The HL7 and related EHR

   (a) Health Information and Data
   (b) Results Management
   (c) Order Entry/Management
   (d) Electronic Communication and Connectivity
   (e) Patient Support
   (f) Administrative Processes
   (g) Reporting and Population Health Management
   (h) Reference Information Model (RIM)
   (i) Vocabulary
   (j) Clinical Document Architecture (CDA)
   (k) Clinical Context Object Workgroup (CCOW)
   (l) Message Transport Specification
   (m) HL7 Services Initiative and collaboration with the OMG Services and Model-Driven Architecture approach

(4) Systematized Nomenclature of Medicine (SNOMED)

(5) Unified Medical Language System (UMLS) (**Table 8-28**)

(6) Public Health Information Network (PHIN)

(7) Pharmacy (**Table 8-29**)

(8) Continuity of Care Record (CCR) (**Table 8-30**)
(9) Patient Health Record (PHR)
(10) Others for possible inclusion (**Table 8-31**)
  (a) Electronic Common Technical Document (eCTD) for Pharmaceuticals
  (b) Electronic Format for Exchange of Individual Case Safety Reports
  (c) Submission of Pharmaceutical Regulatory Information
  (d) Guideline Element Models — GEM-Q
  (e) Cross-Enterprise Clinical Documents Sharing (XDS)

Table 8-7. Web Services Security SOAP Message Security 1.0

Standards Definition Template	
Title	Web Services Security SOAP Message Security 1.0 (WS-Security 2004) March 2004
Category	Security
Objective	The standard enhances the SOAP messaging to provide message integrity and confidentiality. This supports a variety of security models and encryption technologies. It provides a general approach of associating a security token allowing support for multiple token formats. It describes how to encode binary security tokens and describe the tokens associated with a message.
Source: (Standards Body)	Web Services Security Technical Committee www.oasis-open.org/wss
Type	Basic
Versions and Status	Technical Committee Recommendation
Applicability	Allows applications to conduct secure SOAP message exchanges and is used to specify what is often called the SOAP stack. The key features include the following: ■ Supports multiple security token formats ■ Multiple trust domains ■ Multiple signature formats ■ Multiple encryption technologies ■ End-to-end message content security (i.e., not just transport-level security) ■ A flexible set of mechanisms with the focus on a single-message security language with message security
References	Protocol design must address known protocol security issues. Assumes that there are established security sessions, security context, and/or policy agreement.
Relationships to Other Standards	Fits with SOAP 1.1 and SOAP 1.2
Key Terms	

Table 8-8. Liberty Alliance — Federated Approach

Standards Definition Template	
Title	Liberty ID_FF Architecture Overview
Category	Security
Objective	Federated network identity is the key to reducing the friction between the need to share, the desire for autonomy, and the need for clear identity without centralized control. A federated network identity model will ensure that critical private information is used by appropriate parties. Liberty Identity Federation Framework (ID-FF) offers a viable approach for implementing such as single sign-on and federated identities.
Source: (Standards Body)	www.Projectliberty.org
Type	Advanced
Versions and Status	Non-Normative Concept Paper
Applicability	1. Enables users to protect their network identity. 2. Enables independent units to maintain and manage relationships without third-party participation. 3. Provides an open single sign-on standard that includes decentralized authentication and authorization from multiple providers. 4. Creates a network identity infrastructure that supports all current and emerging network-access devices. 5. Defines and manages a *circle of trust* and the operational agreements based on trust relationships. 6. Provides an auditable record of notice and consents that are bound to particular interactions.
References	*Liberty Technical Glossary*
Relationships to Other Standards	
Key Terms	

Standards Definition Template	
Title	Liberty Trust Model Guidelines
Category	Security
Objective	The basic purpose of the document is to define how models of trust can be used among the components defined by other Liberty Alliance standards.
Source: (Standards Body)	Liberty Alliance Project www.projectliberty.org
Type	Conceptual Information
Versions and Status	Non-Normative Guidance Document

Standards Definition Template	
Applicability	Key concepts are defined along with the interaction of key "Liberty components" along with alternative approaches for trust. 1. **Circle of trust environment** defines how a circle of trust is formed based on a series of pairwise trust relationships. 2. **Inter-identity provider interaction requirements** describe the use of active brokering entities as intermediaries to support transactions involving multiple-identity providers. 3. **Glossary of terminology** is summarized below. 4. **Taxonomy of alternatives** is for trust establishment
References	
Relationships to Other Standards	The guidelines and key concepts presented here are especially important in WS-Composite Application Framework (WS-CAF), WS-Business Process Execution Languages (WS-BPEL), and other similar services.
Key Terms	1. **Authentication Enrollment Agreement** represents an agreement between an authentication infrastructure provider and an entity registering in order to be authenticable through the provider's services. 2. **Brokered Trust** describes the case where two entities do not have direct business agreements with each other but do have agreements with one or more intermediaries, so as to enable a business trust path to be constructed between the entities. 3. **Business Agreement** represents an agreement among parties that provides the commercial prerequisites that the parties require in order to engage in business transactions. 4. **Business Anchor** represents an entity with which its holder has a direct business relationship. 5. **Community Trust** applies when the business trust between a part of entities is derived from their enrollment in a common authentication infrastructure and acceptance of its practices without reliance on other business agreement paths. Mutual trust is based on the membership in a community constructed and linked for authentication purposes. 6. **Direct Trust** is obtained when communicating entities hold each other's keys within their Trust Anchor List (TAL), so that their validity is established without reliance on intermediaries. 7. **Indirect Trust** is obtained when communicating entities ascertain the validity of each other's keys based on preexisting trust established with an intermediary, as represented by a trust anchor. 8. **Pairwise Trust** describes the case where two entities have direct business agreements with each other. 9. **Trust Anchor** represents an entity and key that the anchor's holder has determined to trust directly for cryptographic authentication purposes. 10. **Trust Anchor Lists** are maintained by entities accepting cryptographic authentication of other entities, identifying the entities and associated keys that they trust for authentication purposes and upon which validations will be based.

Table 8-9. Security Assertion Markup Language

Standards Definition Template	
Title	Security Assertion Markup Language (SAML) V1.1 & 2.0
Category	Security, Privacy
Objective	SAML defines a framework for exchanging security information between online business partners. SAML defines a common XML framework for exchanging assertions between entities in order to define, enhance, and maintain a standard XML-based framework for creating and exchanging authentication and authorization information.
Source: (Standards Body)	OASIS Security Services Technical Committee www.oasis-open.org/committees/security/
Type	Advanced; 2.0 is Options, Extensions
Versions and Status	Draft 04 — March 30, 2004 SAML 2.0 is also defined with many new features. SAML 2.0 will be used in defining options and extensions.
Applicability	The most pressing need for this standard is to support the problem of a Web single sign-on (SSO) where the users can gain access to Web site resources in multiple domains without having to re-authenticate after initially logging in to the first domain. To achieve SSO, the domains need to form a trust relationship before they can share an understanding of the user's identity that allows the necessary access. Interorganizational Web services drive the standard delivery of security attributes with interorganizational communication. A key element is the definition of metadata for a community or line of business and the ability to exchange that metadata and the related services that are provided.
References	
Relationships to Other Standards	
Key Terms	1. **Asserting Party:** The system or administrative domain that relies on information supplied to it by the asserting party. 2. **Relying Party:** The system or administrative domain that relies on information supplied to it by the asserting parties.

Table 8-10. Metadata for SAML 2.0

Standards Definition Template	
Title	Metadata for SAML 2.0
Category	<Security> <Meta Model Management >
Objective	SAML requires agreements between source and destination sites about information such as URLs, source and destination IDs, certification and keys, and other information in the form of metadata. This standard captures the metadata in a standard format as attributes needed to be used by SAML entities. The entities defined include: Identity Providers, Service Providers, Attribute Authorities, Attribute Consumers, Authorization Decision Authorities, and Affiliate Members.
Source: (Standards Body)	OASIS Security Technical Committee www.oasis-open.org/committee/security/
Type	<Advanced> <Option> <Extension>
Versions and Status	Approved by OASIS March 2005
Applicability	A common cross-organization set of metadata elements will be used for line-of-business and business-line agreements with this being one of the key sources along with UDDI, WSDL, and other metadata sources. Key metadata types include the following: 1. Entity ID Type 2. Key Type 3. Contact Type 4. Extension Type 5. Endpoint Type 6. Localized Name Type 7. Localized URI Type 8. Organization Display Name Type The standards allows an entity to encapsulate all the metadata for all the entities within it that can be exposed (visibility within the community or pair exchanged with) to be shared with others. The provider can be a coordinator, actual organization, or aggregator of a set of services. These are often called domains. The provider will have a unique ID and include an abstract description of its role and its relationship with related identity and service providers or affiliates. The metadata document can be digitally signed along with each item individually signed, specifically the role descriptor and entity descriptors.
References	
Relationships to Other Standards	SAML 2.0 and Metadata Exchange Standard.
Key Terms	

Table 8-11. Enterprise Privacy Authorization Language

Standards Definition Template	
Title	Enterprise Privacy Authorization Language (EPAL)
Category	<Service Definitions> <Messaging> <Data Access> <Resources> <Security> <Privacy> <Business Process> <Reliability> <Meta Model Management>
Objective	EPAL goes beyond an application and lays out a standard to protect customers' and citizens' privacy information enterprisewide. Customer and citizen information must be protected based on a global enterprisewide privacy policy. The enterprise privacy policy defines a set of rules where each rule can allow a set of data users to perform an action in a set of actions on a category in a set of categories for any purpose(s).
Source: (Standards Body)	EPAL was developed by IBM and has been turned over the OASIS.
Type	<Advanced> <Option> <Extension>
Versions and Status	Draft Standard Some missing information that will be needed to handle line-of-business and federated inter-enterprise (interprise) conflicts between organizational policies that are engaged in business transactional data exchanges.
Applicability	
References	
Relationships to Other Standards	
Key Terms	

Table 8-12. Trust Model Guidelines

Standards Definition Template	
Title	Trust Model Guidelines
Category	<Security>
Objective	This standard takes the Liberty Alliance Trust Guidance and has it reviewed by a broader, more inclusive community. Most of concepts are the same as the earlier Liberty Alliance Trust Guidelines. Differences will be highlighted.
Source: (Standards Body)	OASIS Security Services Technical Committee
Type	<Conceptual>

Standards Definition Template	
Versions and Status	Draft
Applicability	Same as the Liberty Trust Guideline document
References	
Relationships to Other Standards	This is the next generation of the Liberty Trust Model. It was initially accepted as-is and an action item review list was created.
Key Terms	

Table 8-13. X.509 Attribute Certification — Public Key Infrastructure

Standards Definition Template	
Title	X.509 Attribute Certificates- PKI Proxy Certificate Profile
Category	<Security and Privacy>
Objective	This standard describes how communities can share policies and authorization schemes based on sharing attributes known as proxy credentials. It enables entity A to grant to entity B the right to be authorized with others as if it were A. This profile provides a framework for carrying policies in Proxy Certificates that allows proxying to be limited through.
Source: (Standards Body)	Internet Engineering Task Force (IETF) — Network Working Group RFC 3820 June 2004. www.ietf.org
Type	
Versions and Status	In RFC review status. Many of the concepts have been developed within the Grid Services Community Authorization Services and a series of related projects.
Applicability	The standard can enable the policies among business partners within a channel to be defined and shared in a consistent manner with trust of the certificate authority. The design center hub will act as the certificate authority.
References	1. Butler, R., Engert, D., Foster, I., Kesselman, C., and S. Tuecke, “A National-Scale Authentication Infrastructure”, *IEEE Computer,* vol. 33, pp 60-66, 2000. 2. Farrell, S. and R. Housley, “ Internet Attribute Certificate Profile for Authorization”, RFC 3281, April 2002. 3. Foster, I., Kesselman, C., Tsudik, G., and S. Tuecke, “A Security Architecture for Computation Grid”. 4. www.globus.org sections on Grid Security Infrastructure Community Authorization Services Guideline documents
Relationships to Other Standards	

Standards Definition Template	
Key Terms	**Certificate Authority (CA)** **End Entity Certificate (EEC)** **Public Key Certificate (PKC)** **Attribute Authority (AA)** **Proxying** is used to solve two related problems: single sign-on and delegation where a remote resource needs to perform a service in behalf on the user. **Proxy Certificate (PC)** is an X.509 public key certificate with the following properties: 1. It is signed by either an X.509 EEC or another PC. This EEC or PC is referred to as the *proxy issuer* (PI) 2. It can sign only another PC. It cannot sign an EEC. 3. It has its own public and private key pair, distinct from any other EEC or PC. 4. It has an identity derived from the identity of the EEC that signed the PC. When a PC is used for authentication, in may inherit rights of the EEC that is signed the PC, subject to the restrictions that are placed on that PC by the EEC. 5. Independent identity issues in conjunction with attribute assertion. 6. X.509 is extended to identify the PC and to place policies on the use of the PC. **Attribute Certificate (AC)** can be used to grant to one identity, the holder, some attributes such as a role, clearance level, or alternative identity such as “charging identity” or “audit identity” or membership within a channel or community.

Table 8-14. Electronic Health Records Security

Standards Definition Template	
Title	Electronic Health Records (EHR) Security
Category	<Security> <Privacy>
Objective	EHR-specific security considerations
Source: (Standards Body)	
Type	
Versions and Status	
Applicability	
References	ISO/IEC 17799:2000 “Information Technology Code of Practice For Information Security Management”
Relationships to Other Standards	
Key Terms	

Table 8-15. SQL 2004

Standards Definition Template	
Title	SQL 2003
Category	
Objective	International Standard Replacing SQL:1999
Source: (Standards Body)	www.ansi.org
Type	
Versions and Status	Makes revisions to all parts of SQL:1999 and adds a brand new part 14:SQL/XML (XML-Related Specifications) ISO/IEC 9075-14:2003 Information Technology-Database languages-SQL- Part 14: XML-Related Specification (SQL/XML) A substantial chunk of SQL:1999's Part 2: Information Schema and Definition Schema is split into a separate part, Part 11: SQL/Schemata in SQL:2003. SQL:1999's Part 5:SQL/Bindings has been eliminated in SQL:2003 by merging all the material contained in that part into SQL:2003 Part 2: SQL/Foundation.
Applicability	SQL/XML New Features ■ Mapping SQL tables, schemas, and catalogs to XML documents ■ Generation of an XML schema corresponding to an XML document generated from SQL data ■ An XML data type to allow columns of SQL tables to contain XML data ■ Publishing functions that allow application writers to create XML directly within SQL queries, including such functions as XMLELEMENT, XMLATTRIBUTES, XMLFOREST, XMLCONCAT, XMLAGG, and XMLGEN New features: ■ New data types — Eliminates BIT and BIT Varying and adds three new data types: BIGINT, MULTISET, and XML ■ Enhancements to SQL-invoked routines ■ Extensions to CREATE TABLE statements ■ A new MERGE statement ■ A new schema object — the sequence generator ■ Two new sorts of columns: identity columns and generated columns ■ Retrospective check constraints ■ Online Analytical Processing (OLAP) extensions in the form of new built-in functions (both scalar functions and aggregate functions) ■ WINDOW clause in query expressions (published previously as an Amendment to SQL:1999) ■ Support for the use of sampled data for better performance, improved savepoint handling, and enhanced diagnostics
References	Database Languages-SQL, ISO?IEC 9075-*, 2003
Relationships to Other Standards	Replaces SQL 1999
Key Terms	

Table 8-16. Core Extensible Markup Language

Standards Definition Template	
Title	Core Extensible Markup Language (XML) Standards
Category	XML Core Standards have an overall impact on all Solution Sets
Objective	The core XML standards are foundation standards that are fundamental to all the other new standards and applications that can be built upon them.
Source: (Standards Body)	Core Standards consist of the following: ■ XML 1.0 W3C Recommendation – 1998 ■ Namespaces in XML — W3C Recommendation – 1999 ■ XPath — W3C Recommendation – 1999 ■ XBase — W3C Recommendation – 2001 ■ XLink — W3C Recommendation – 2000 ■ XPointer — W3C Working Draft – 2001
Type	
Versions and Status	These set of standards are relatively stable and widely supported by XML parsers and tools.
Applicability	■ **XML 1.0** establishes the rules for how XML documents can be constructed and how they can be encoded using various character sets. All other standards are in some way linked to this standard and its extensibility. ■ **Namespaces** in XML provide support for mixing the vocabularies from multiple XML applications into a single document. ■ **XPath** serves as one of the key elements in document manipulation by providing a capability to identify locations within and provide the capability to portions of XML documents. ■ **XBase** allows the override of the default base for a relative URLs with an explicit base. ■ **XLink** is one of the key pieces that will need to be refined to link to higher level elements such as the Semantic Web. ■ **Xpointer** provides the capability to locate single points or ranges of points within a document. It defines how Xpath expressions may be used to locate XML document nodes.
References	www.w3c.com Many books are available such as Strategic XML, by W. Scott Means, SAMs, 2002. www.xml.org — Robin Covers Pages provide excellent overview of both standards and vendor progress in meeting those standards.
Relationships to Other Standards	This set of core XML Standards are a basic building block for all elements.
Key Terms	

Table 8-17. Standard XML Application Elements

Standards Definition Template	
Title	Standard Extensible Markup Language (XML) Application Elements
Category	Data Management and Data Sharing and Service Interoperability and Business Area Improvements will depend on these fundamental Standard XML Application elements.
Objective	These sets of standard application elements are intended to be used by other developers who are building their own special-purpose application.
Source: (Standards Body)	Standard XML Applications consist of the following: ■ Extensible Stylesheet Language (XSL) ■ XSLT ■ XSL Formatting Objects (XSL-FO) ■ XML Schema ■ Resource Description Framework
Type	<Advanced>
Versions and Status	These standards are emerging, but they are stable and beginning to be supported by all the major vendors and many smaller entrepreneur.
Applicability	
References	www.w3c.com Many books are available such as Strategic XML, by W. Scott Means, SAMs, 2002. www.xml.org — Robin Covers Pages provide excellent overview of both standards and vendor progress in meeting those standards.
Relationships to Other Standards	These application support tools will grow more as new problems are addressed in the translation.
Key Terms	

Table 8-18. Cannon XML

Standards Definition Template	
Title	Cannon XML
Category	
Objective	
Source: (Standards Body)	■ www.w3c.org
Type	<Basic>
Versions and Status	Version 1.0 March 15,2001
Applicability	
References	
Relationships to Other Standards	
Key Terms	

Table 8-19. Exclusive XML Canonicalization

Standards Definition Template	
Title	Exclusive XML Canonicalization
Category	
Objective	
Source: (Standards Body)	■ www.w3c.org
Type	<Basic>
Versions and Status	Version 1.0 July 18, 2002
Applicability	
References	
Relationships to Other Standards	
Key Terms	

Table 8-20. XML Scheme

Standards Definition Template	
Title	XML Schema
Category	
Objective	
Source: (Standards Body)	
Type	<Basic>
Versions and Status	
Applicability	
References	
Relationships to Other Standards	
Key Terms	

Table 8-21. SQL/XML 2003

Standards Definition Template	
Title	SQL/XML 2003
Category	
Objective	
Source: (Standards Body)	■ www.ansi.org
Type	<Basic> International Standard

Standards Definition Template	
Versions and Status	Version ISO/IEC 9075-14:2003 Information Technology — Database languages-SQL- Part 14: XML-Related Specification (SQL/XML)
Applicability	■ Mapping SQL tables, schemas, and catalogs to XML documents ■ Generation of an XML schema corresponding to an XML document generated from SQL data ■ An XML data type to allow columns of SQL tables to contain XML data ■ Publishing functions that allow application writers to create XML directly within SQL queries, including such functions as XMLELEMENT, XMLATTRIBUTES, XMLFOREST, XMLCONCAT, XMLAGG, and XMLGEN
References	
Relationships to Other Standards	
Key Terms	

Table 8-22. XSLT

Standards Definition Template	
Title	XMLT
Category	
Objective	
Source: (Standards Body)	■ www.w3c.org
Type	<Basic>
Versions and Status	
Applicability	
References	
Relationships to Other Standards	
Key Terms	

Table 8-23. XQuery

Standards Definition Template	
Title	XQuery
Category	
Objective	
Source: (Standards Body)	■ www.w3c.org
Type	<Basic>
Versions and Status	Version
Applicability	

Standards Definition Template	
References	
Relationships to Other Standards	
Key Terms	

Table 8-24. XQuery API for Java

Standards Definition Template	
Title	Query API for Java
Category	
Objective	
Source: (Standards Body)	■ www.w3c.org
Type	<Basic>
Versions and Status	Version
Applicability	
References	
Relationships to Other Standards	
Key Terms	

Table 8-25. GGF Data Access and Integration Services

Standards Definition Template	
Title	GGF DAIS (Data Access and Integration Services)
Category	The Global Grid Forum (GGF) is producing technical specification to enable both relational and XML databases to be located, accessed, and replicated in this environment.
Objective	The objective is to produce a specification that describes a service-based interface for accessing and integrating data in existing relational and XML databases on the grid.
Source: (Standards Body)	■ www.gridforum.org/6_DATA/dais.htm
Type	<Basic>
Versions and Status	

Standards Definition Template	
Applicability	■ **Virtualizing data** in the grid means applications are able to discover, access, and update data irrespective of the format of the data located in the grid. ■ **Managing data** in the grid means making sure data is available to applications with appropriate performance characteristics in the grid environment. ■ **Integrating data** with the grid infrastructure means making sure that data management systems support the mechanisms of the grid. ■ These features are implemented outside the database systems themselves. They allow for a common representation of the database management systems and a common resource representation. They define a data-access session and the relationship between the client and the data resources, and they support the data requests that contains SQL, XPath, or XQuery. ■ It defines the output results format of the data sets created, including features for the following: – Naming results for subsequent use – Multiple results formats – Chunking large quantities of data – Asynchronous delivery of results – Delivery of results to third parties.
References	
Relationships to Other Standards	
Key Terms	

Table 8-26. Storage Management Initiative Specification

Standards Definition Template	
Title	Storage Management Initiative Specification
Category	
Objective	
Source: (Standards Body)	■ www.snia.org
Type	<Basic>
Versions and Status	Version
Applicability	
References	
Relationships to Other Standards	
Key Terms	

Table 8-27. HL7 Standards

Standards Definition Template	
Title	HL7 Standards
Category	Health Level 7 messaging standards ensure that each Federal agency can share information, which will improve coordinated care for patients in such areas as entries of orders, scheduling appointments and tests, and better coordinating the admittance, discharge, and transfer of patients.
Objective	
Source: (Standards Body)	
Type	<Basic>
Versions and Status	
Applicability	
References	
Relationships to Other Standards	
Key Terms	

Table 8-28. HIPAA Code Sets Master Index

Standards Definition Template	
Title	Medical Code Sets_HIPAA Code Sets Master Index
Category	
Objective	
Source: (Standards Body)	
Type	<Basic>
Versions and Status	
Applicability	
References	
Relationships to Other Standards	
Key Terms	

Table 8-29. National Council on Prescription Drug Programs

Standards Definition Template	
Title	National Council on Prescription Drug Programs (NCPDP)
Category	NCPDP standards apply to ordering drugs from retail pharmacies, and they standardize information between healthcare providers and the pharmacies.
Objective	
Source: (Standards Body)	
Type	<Basic>
Versions and Status	
Applicability	
References	
Relationships to Other Standards	These standards have already been adopted under HIPAA and ensure that non-HIPAA programs use the same standards.
Key Terms	

Table 8-30. Continuity of Care Record

Standards Definition Template	
Title	Continuity of Care Record (CCR)
Category	
Objective	
Source: (Standards Body)	
Type	<Basic>
Versions and Status	
Applicability	
References	
Relationships to Other Standards	
Key Terms	

Table 8-31. Digital Imaging Communications in Medicine

Standards Definition Template	
Title	Digital Imaging Communications in Medicine (DICOM)
Category	DICOM standards enable images and associated diagnostic information to be retrieved and transferred from various manufacturers' devices as well as medical workstations.
Objective	

Standards Definition Template	
Source: (Standards Body)	
Type	<Basic>
Versions and Status	
Applicability	
References	
Relationships to Other Standards	These standards have already been adopted under HIPAA and ensure that non-HIPAA programs use the same standards.
Key Terms	

Business Enabling Technologies

1. Business Process Management — BPMN, BPEL, etc.
2. Business Forms Management — Xforms
   a. XML Forms (**Table 8-32**)
   b. Business Rules, rules standardization efforts, Rule Markup Language (RuleML)
   c. Workflow Management Coalition (WFMC)
   d. Business Protocols — BPSS from ebXML
   e. CRM-XRM
   f. Universal Business Language (UBL) and Core Components

Table 8-32. XForms

Standards Definition Template	
Title	XForms
Category	
Objective	
Source: (Standards Body)	
Type	<Basic>
Versions and Status	
Applicability	
References	
Relationships to Other Standards	
Key Terms	

Performance Measurement

Key concepts for this area are based on the Balanced Scorecard and Performance Prism Government results initiatives. There are efforts in this area at the Federal and State levels and with the healthcare and other communities that involve the following: transaction processing, IT infrastructure, call centers, etc. A set of "near-fit" standards will be defined and common "good practices" will be created within MITA communities.

1. Performance Dashboard and Scorecard Structure (none available)
2. Performance Measurement Library Elements, which are derived from the following:
   a. GPRA
   b. GSAC
   c. FEA PRM
   d. PARTS
3. IT Service Management Capability Maturity Model, candidates for elements considered in the Performance-Based Set of Services
4. Look at existing Medicaid Reporting Requirements and look at the DSS system requirements in some of the most recent RFPs
5. Healthcare Metrics
   a. Healthcare Patient Safety Measures
   b. Health Plan Employer Data and Information Set (HEDIS)
   c. Build upon the healthcare metrics product specification (e.g., AdvanceMed CompareCare, Kelsey Rauch and Dale Prestipino, Clinical Data)
   d. Performance Soft

Flexibility: Adaptability and Extensibility

There are limited standards efforts in this area, but there is extensive work in model-driven, declarative programming by both vendors and academics.

1. Design for change and management of change. Aspects include oriented design processes. Language-level tools now moving to design and model level
2. Event alerting over the Internet (WS-Eventing and WS-Notification)
3. Situated agents based on Foundations of Intelligent Physical Agents (FIPA) standards
4. WSDM — one of the most important standards in this areas
5. ITIL
6. DMTF Standards
7. Design for Change guidelines or UML stereotypes needed.

Operations and Management

1. Web Services Resource Framework (WSRF)
2. Web Services Remote Portlets (WSRP)
3. WSRM
4. ebXML-Collaborative Protocol Profile and Agreement (CPP/A)
5. Automated Deployment Services
6. Web Services for Management Extensions (WMX), a framework for end-to-end server management
7. Platform Management Architecture
    a. DMTF Server Management Workgroup (www.dmtf.org)
    b. CIM/WMI
    c. Simple Network Management Protocol (SNMP)
    d. Intelligent Platform Management Interfaces (IMPI 2.0 Firmware)
    e. OSA/IPMI Core
        (1) www.intel.com/design/servers/ipmi/ipmi.html
        (2) Enable cross-platform management system
        (3) Common interfaces and abstraction
    f. Web Services for Management (WS-Management)

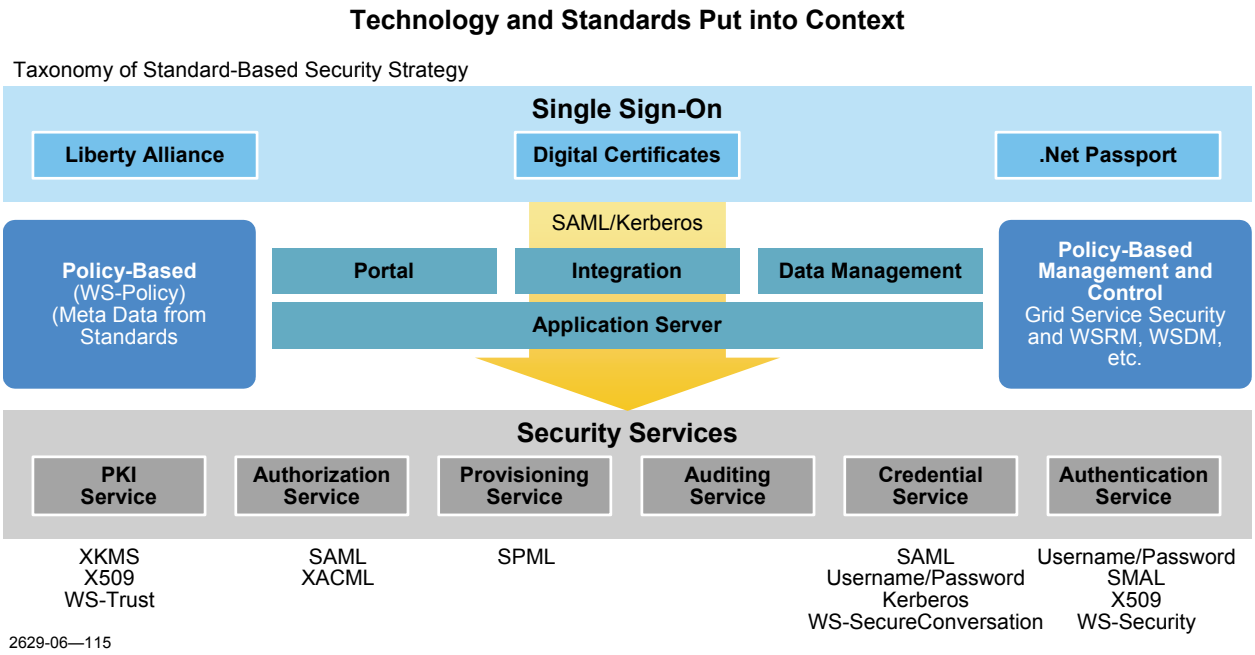

Figure 8-3. Technology and Standards Put into Context

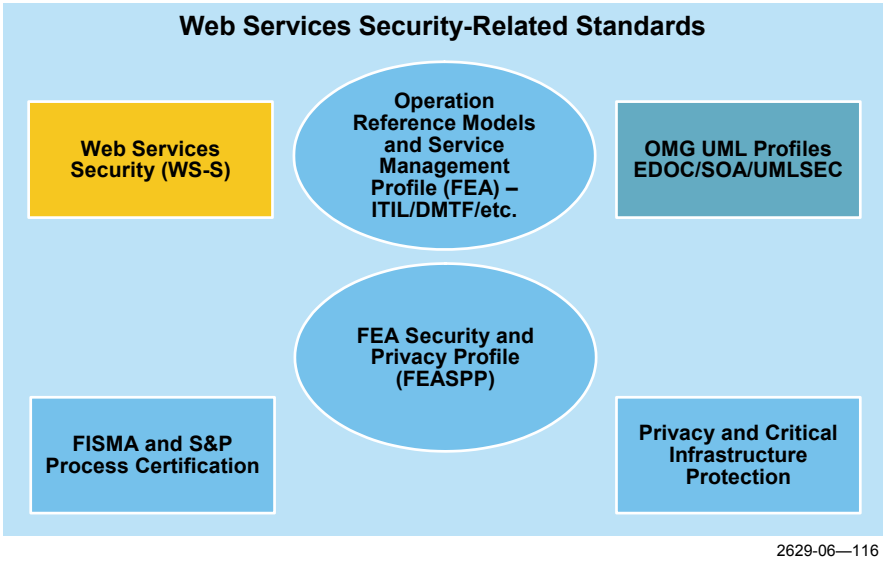

Figure 8-4. Web Services Security–Related Standards

This page intentionally left blank.