# Part III — Technical Architecture

# Chapter 7 — Application Architecture

## Introduction

Previous chapters discussed Medicaid IT Architecture (MITA) Business Services (Part III Chapter 4) and Technical Services (Part III Chapter 6). MITA services are central to MITA but do not provide an integrated solution by themselves. For example, they do not by themselves eliminate the need for middleware and many traditional technologies or provide a mechanism for application integration. They do, however, provide a mechanism that lets different architectures use components.

This section discusses the MITA Application Architecture (AA), which is a component of MITA's Technical Architecture (TA). MITA approaches application integration using a service-oriented architecture (SOA), beginning with application design and operations and adapting them to changing needs. MITA business services are new but not radical. MITA integrates its business services with its technical services through service elements that States can configure as a service layer. Using SOA as an integrating framework allows MITA services to remain both platform independent and technology independent and yet remain interoperable.

> MITA provides platform- and technology-independent services by only specifying their message structure, the business logic of the service, and the abstract portion of the service's interface. States are responsible for defining the concrete portion of the service's interface based on their specific implementations.

This chapter answers the following questions:

- What is the MITA Application Architecture?
- What are the key components of the MITA Application Architecture?
- How do MITA services interact with the MITA infrastructure?
- How do States use the MITA Application Architecture?
- How do States participate in developing the MITA Application Architecture?

### Purpose

The MITA AA defines the relationship between end users, MITA services, and the MITA infrastructure. It also provides guidance and specifics to State Medicaid IT staffs on how to connect their services and infrastructures with those of MITA to improve services for end users.

### Scope

The current version of the MITA Framework discusses concepts and high-level details of the AA. Future versions will include specific AA details and requirements.

MITA AA goals include the following:

- The AA will create the infrastructure States need to use MITA services effectively.
- The AA will map technology standards to components.
- The AA will define patterns for components that States will use as templates for their implementations and will store details on those implementations for other States to share. The AA will not address implementation specifics, such as commercial off-the-shelf (COTS) products, specific performance metrics (e.g., bandwidth or MIPS), software components, or object classes.
- The AA will be extended as necessary to be compatible with electronic health records after they are defined.
- The AA will not contain information on a State's unique processes and infrastructure. Rather, the State will supplement the AA with its unique requirements.
- The AA will not contain information on States' physical networks and hardware. Rather, States will develop their specific physical networks and hardware based on their implementation programs.

## What Is the MITA Application Architecture?

The MITA AA connects MITA business services with MITA technical services, as shown in **Figure 7-1**, using its AA.

States will tailor MITA business services to their needs. Business services will have a common core for all MITA processes but can be adapted and extended to meet States' special policies, rules, and deployment environment, including the types of service infrastructure and technical services States require. MITA will define its services from the abstract level to the implementation-guide level, which will allow States to build service interfaces as standard interfaces without dialects caused by interpretations. (MITA business services are discussed in Part III Chapter 4; MITA technical services are discussed in Part III Chapter 6.)

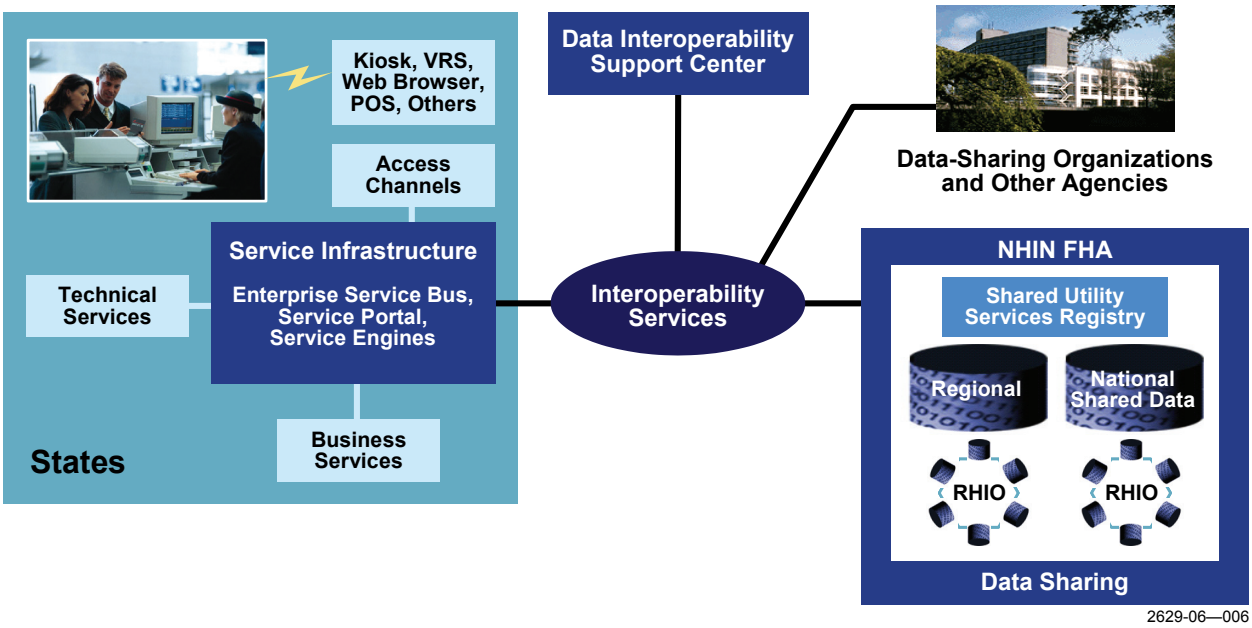



*Figure 7-1. Conceptual Technical Architecture Diagram*

The service infrastructure will use standards-based elements that will allow intra-State service process integration and data sharing with other organizations and agencies. MITA will be compatible with the Federal Health Architecture (FHA), the National Health Information Network (NHIN), regional and national shared data sources, and the network on Regional Health Information Organizations (RHIOs). MITA has defined a series of interoperability services based on Web Services (WS) and XML message formats and protocols. The tools States need to establish interoperability, data capabilities, and other support needs are available individually, to States in groups using common facilities, and in other ways. The following sections provide a drilldown of the top-level MITA SOA. They describe key infrastructure components, such as the Enterprise Service Bus (ESB), the service management engine (SME), and infrastructure services (e.g., external data-sharing hubs, interoperability channels, and data management services), and provide references to standards they use.

## Parts of the MITA Application Architecture

This section identifies the parts of the AA. A multilayer AA model represents a combination of MITA applications and connections to deliver services to stakeholders, as shown in **Figure 7-2**. The four levels are the Access Layer, the Service Management Layer, the Service Application Layer, and the Platform Layer.

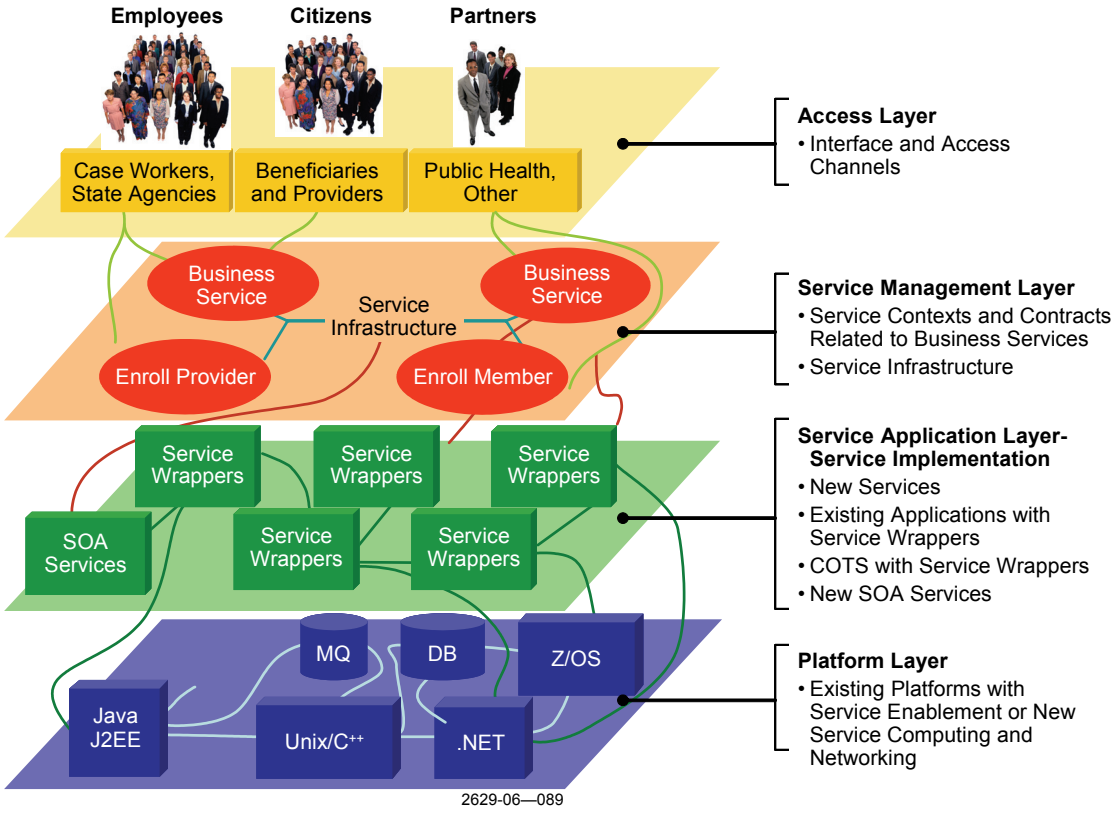



*Figure 7-2. Multilayer Application Architecture Model*

**Access Layer.** The Access Layer contains the touch points that connect stakeholders through their roles and tasks to the sets of services they need to perform those roles and tasks. There will be interfaces with more capabilities for employees with services that are specific to one or more roles to which the employee is assigned. Nonemployees will have access to fewer services and cannot look at information other than their own or information on persons for whom they are providing support by proxy. Partners' interfaces will also be restricted to agreed-upon business agreements/business service contracts for information exchanges, sharing, and specific services.

**Service Management Layer.** The Service Management Layer consists of the service infrastructure, service contexts, and service contracts for each business service (Enroll Member, Enroll Provider, etc.) and provides a view into business services as they relate to roles and task assignments. (See details below.) The Service Management Layer will be linked to the application layers discussed below, either directly or through service wrappers.

**Service Application Layer.** The Service Application Layer consists of services that make up a State Medicaid operations enterprise. Although the MITA Service Application Layer consists of services, those services might be new services, wrapped legacy applications, or wrapped COTS products. New services will be defined and integrated with business services and technical services and with sub-business services, with linking and binding to the service infrastructure.

The Service Application Layer will evolve incrementally. Applications can run on the same platforms, with new features that will allow them to be service enabled while some new service computing and service networking capabilities are being provided.

**Platform Layer.** Most service platforms can be service enabled, and new service-computing capabilities and new service-oriented networks can evolve, depending on the performance and reliability needs of each State. MITA will standardize the Access Layer, the Service Management Layer, and the service wrapper definitions of the Service Application Layer. States will be responsible for the Platform Layer and for defining the implementation within a service wrapper in the Service Application Layer. MITA will store metadata about these State implementations in the MITA repository.

## What Are the Key Components of the MITA Application Architecture?

The relationship between the MITA infrastructure and MITA services is shown in **Figure 7-3**. Business services and technical services are linked by service infrastructure elements using the key integration element known as the ESB. David Chappell in *Enterprise Service Bus* (O'Reilly Media, 2004) describes an ESB as "a standards-based integration platform that combines messaging, Web services, data transformation, and intelligent routing to reliably connect and coordinate the interaction of significant numbers of diverse applications across extended enterprises with transactional integrity." It should be noted that there is currently no universal agreement within the industry regarding the components and functionality of an ESB. MITA's concept of an ESB follows Chappell's definition. MITA has included common elements and those critical to linking business services and technical services. The service integration and interoperability methods provide loose connectivity (they are often called *loosely coupled*) and are key enablers of flexibility. The consistent use of this service approach is a key element to implementing the SOA. The key components of the MITA AA are:

- ESB and access channels
- Service management engine
- Service gateways and mediators
- Business services
- Technical services
- Performance management
- Service interoperability
- Security and privacy (S&P)

These components are discussed in the sections that follow.

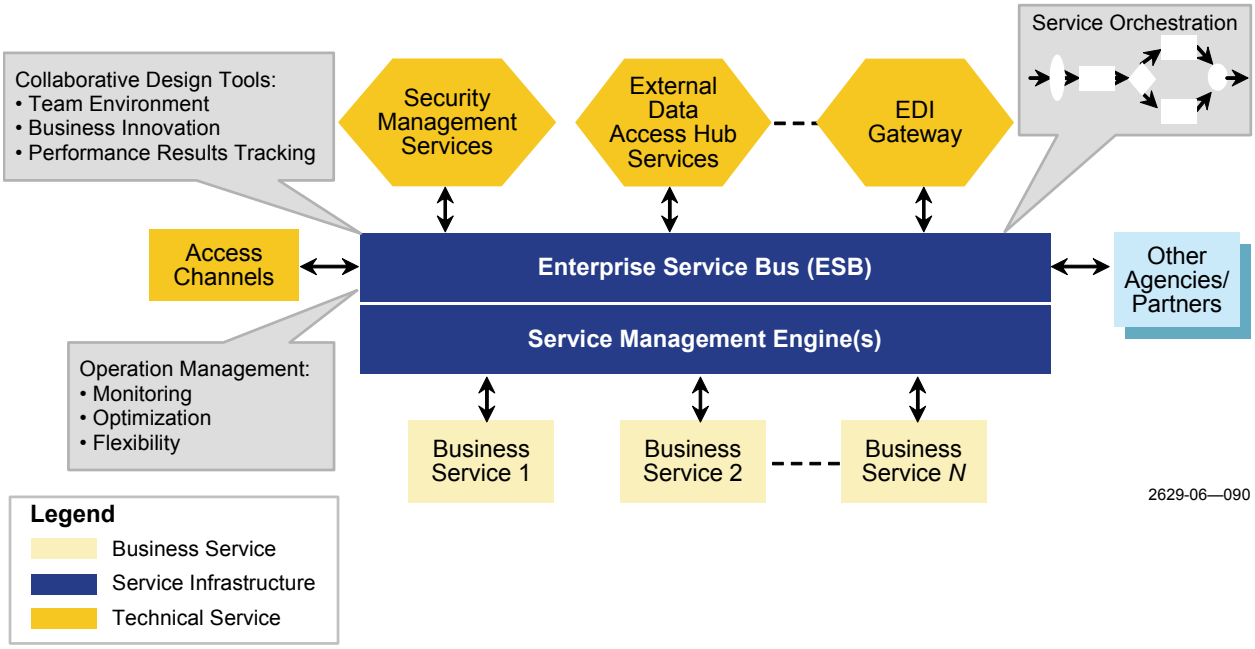



*Figure 7-3. Service Infrastructure*

## Enterprise Service Bus and Access Channels

Traditionally, users accessed or linked to systems using proprietary formats of individual vendors, developers, or integrators, which make systems more complex and hinder interoperability and integration. MITA addresses this issue through Access Channel Services, shown in **Figure 7-4**. Access Channel Services provide the specific device handling types. Initially, the focus has been on five different device types and related technical services, although the types of devices will evolve and change and MITA will add new access channels and eliminate outmoded ones. The unique features of each device will be handled by each Access Channel Service.

The access channel routing and management capability will tie in to the security boundary protection services, access other S&P services that support single sign-on needs, authenticate users, set up the role-based access control (RBAC) permission, and pass a token (or link) to the ESB. The token will be used with the ESB and passed to the business service area with any correlated information (often called a *correlation set*) that relates the service message to the problem domain (often called the *context of the problem* and the *context of the user*). Correlation sets can be carried along entirely, but more often a small token to the correlation set information is provided. The ESB or a technical service will have the capabilities for logging and gathering levels of tracking information for exception handling, recovery, and S&P auditing.

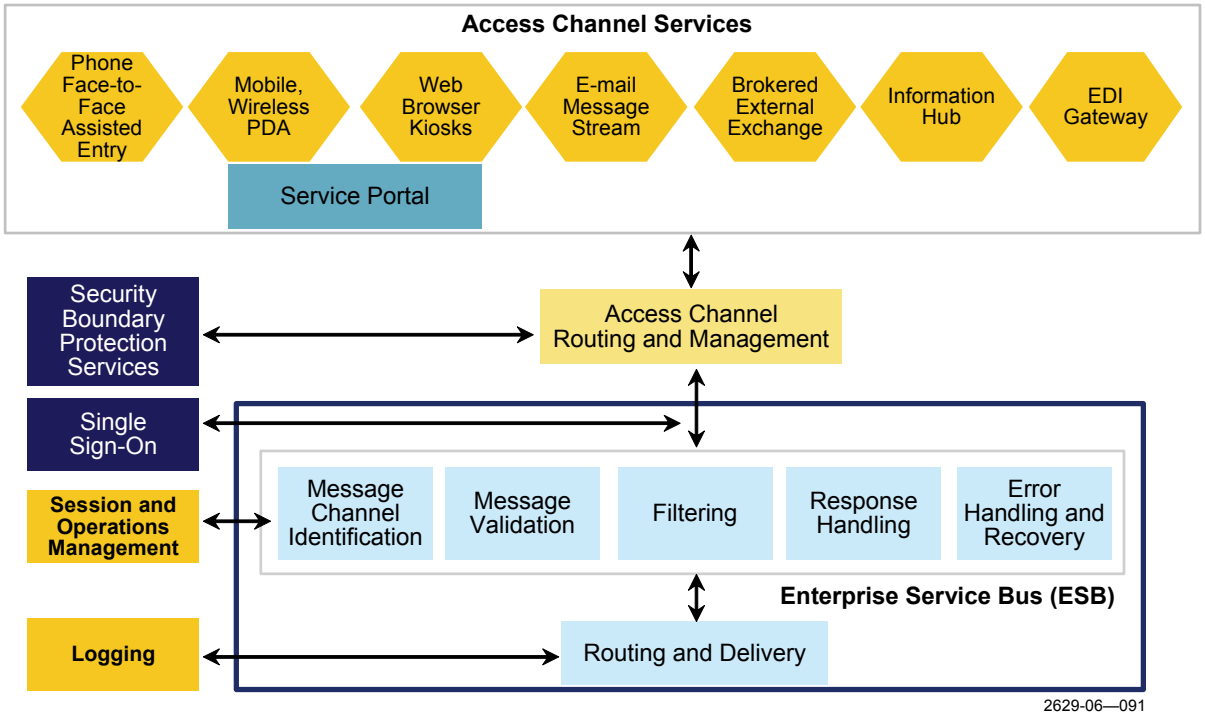



*Figure 7-4. Enterprise Service Bus and Access Channel Services*

Access Channel Services and the ESB are designed to fit a range of interoperability issues across business areas to provide cross-organization interoperability services. Access Channel Services are defined to handle specific device types. Initially, MITA has focused on five different device types and related technical services, although the types of devices will evolve and change and MITA will add new access channels and eliminate old ones. An access channel provides the translation from the unique features of the device and technology, such as the size of the screen and the layout of the keys, to translate the message to a common format handled by the ESB. The access channel routing and management capability will tie in to the Security Boundary Protection Services and can access other S&P services that support single sign-on needs.

Passing a large amount of information is a performance burden. One technique used to reduce this burden is to create a small token for providing the S&P rights information for specific sign-on. The boundary services pick up the initial token as the message enters the ESB. The user signs in and goes through an authentication process (similar to eAuthentication, a General Services Administration-provided government component), and RBAC is verified. The service can add additional information to the token. For example, if the user is returning to previously uncompleted work, adding correlation data to the token will allow the user to start where he or she left off.

Many organizations have Web portals to facilitate access to their systems. (A service-enabled Web portal is called a *service portal*.) The other major element of the service portal is the integrated manager of the human side of the workflow. The service portal can handle the work

queues involved in each user's role(s). One user may have a clear role and needs only one work queue, while others may have multiple roles. Service portals follow WS standards, such as WS-RemotePortlet standards. Services users can access services that provide a path between their work queues and other special areas (e.g., alerting) to form a service connection, with each work queue representing one end of the service endpoints and the business services representing the other end. The service endpoints are essentially a uniform resource identifier (URI) for service users and service providers, and the ability to connect in a standardized ways is one of the key uses of the service portal. MITA will use WS-Addressing standards for the service endpoints. The service portal represents a natural evolution of the Web portal technology. It has new capabilities that allow it to interface with the other service infrastructure components. Some of the key capabilities of a Web portal are that it supports Web browsers that understand Web Service Definition Language (WSDL) and sends outputs to other service elements with service-formatted messages. The portal and portions of the portal are service endpoints. A service endpoint is a URI pointer to the service provider and the service user, as defined in WS-Addressing.

**Figure 7-5** shows how security tokens are integrated into the infrastructure.

The user will sign on and go through an authentication and authorization process, which consists of the following steps:

1. The security service creates a token (similar to an identification) for providing S&P rights, depending on the specific sign-on. An RBAC is then created.
2. The token tells the ESB the message can be transmitted and the connection made to the proper business service.
3. The business service initiates correlation sets, registers the correlation token, and tracks progress through the business service. The user can stop or pause and sign on the next day. If there is a failure, the recovery can identify the progress, based on the token and the corresponding correlation set.
4. The technical and business services can use the token to determine access control to business logic and data access.

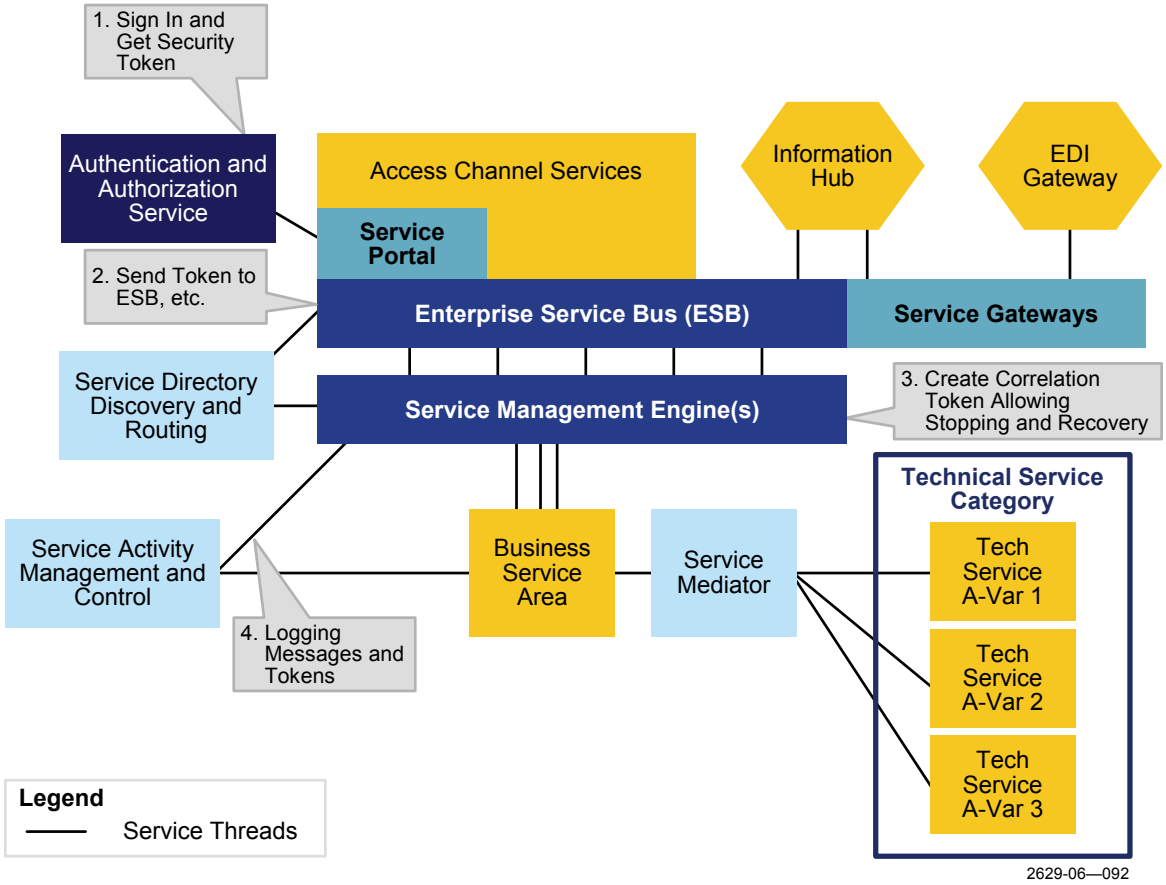



***Figure 7-5. Service Infrastructure's Operation Concept of Security***

## Service Management Engine

A second key part of the MITA application infrastructure is the SME, shown in **Figure 7-6**. Currently, the industry does not distinguish between the capabilities of SMEs and those of ESBs. The Organization for the Advancement of Structured Information Standards (OASIS) is currently defining a standard for SOA infrastructure, which MITA will incorporate into a future release of the MITA Framework. Until then, States should review the combined capabilities of their ESBs and SMEs. SMEs, which are mini-operating systems for services, manage the execution of the business services and technical services.

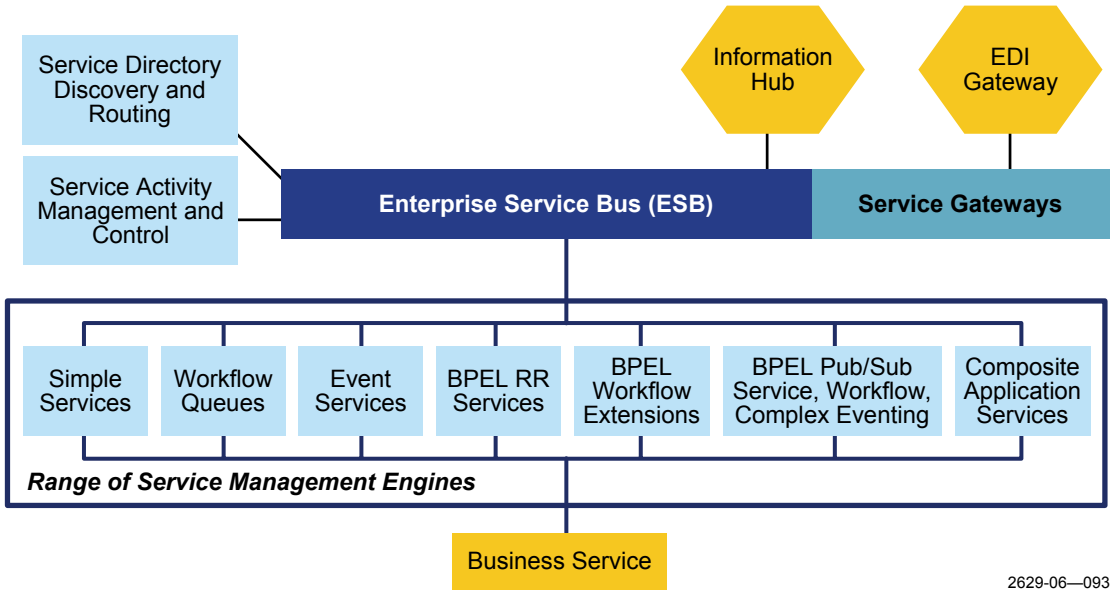



*Figure 7-6. Service Infrastructure — Service Management Engine*

SMEs execute the service contracts defined in WSDL or the more advanced service composition and business process management languages. These engines come in many sizes and shapes and support a range of capabilities. Different services will have different service behavior needs, from very simple services to complex and composite services. Depending on a State's need, the business service will use different orchestrations and management of services. Seven types of service engines can provide this orchestration and management:

- **Simple Services.** Service specification with a service contract, as defined in WSDL, and a simple request of a service and response.
- **Workflow Queues.** Services performed primarily by people, in which messages or cases are routed to a specific worker or group of workers who would normally handle that case. A queue of messages and cases is the work that needs action by a person or role. Each person will have a queue of work.
- **Event Services.** Services that manage the delivery of event messages to several business services and people/roles/contexts interested in a condition and change of behavior of interest.
- **Business Process Execution Language Engine with Request Response.** A service that triggers a Business Process, as defined in WS-Business Process Execution Language (WS-BPEL 2.0 standard), using a triggered message in a simple request–response message pattern, as defined in WS-BPEL 2.0 standard. The business process will be executed and the result will be sent to the locations identified in the Business Process Model.
- **BPEL with Workflow Extensions.** A service that combines BPEL (with its strong focus on automating human decisions and actions) with an ability to integrate the

workflow queuing and high levels of workflow management. A common bridge between BPEL and workflow tools is being defined by the Workflow Management Coalition (WFMC) standards group (Level 4).

- **BPEL Advanced.** A service (currently proposed) that will include more advanced BPEL features (Pub-Sub, Service Plus, Workflow, and Complex Eventing). Although it should be considered, one should be cautious about "locking in" with a specific vendor's implementation (Level 4).
- **Composite Application Services.** Services that address more comprehensive business processes and how to handle transactions, people involvement, and long-running activities. The WS Composite Application Framework standard addresses these needs (Level 4).

Marketed products exist in each of the above categories. More innovation will come over the next few years, and vendors will have "new" features that might help but might also create incompatibilities. SMEs are a key aspect of "designing and managing for change," a key part of MITA's goal of flexibility.

The MITA team expects that more capabilities and new patterns of business processes and workflow will be defined and is designing the MITA structure to be open to those changes. For example, some systems are intended for multiple users who collaborate around a business process (called *human interaction management systems*), rather than for just one user. Other process metric management systems have more built-in decision support and reactivity. These capabilities may be Level 4 or 5 in our technical capability structure.

## Service Gateways and Mediators

To deliver services end to end, MITA needs not only a common set of service elements that will agree with set standards, but also bridging technologies that will address changes and innovation. Those bridging technologies should be semiautomated and sufficiently intelligent to handle many of the common interoperability elements, as shown in **Figure 7-7**. Two service elements are defined — the Service Gateway and Service Mediators — and additional capabilities may be needed. MITA needs bridging services to mediate differences because absolute compliance with standards is not realistic.

Service Gateway addresses external or cross-boundary compatibilities between ESBs. The Service Gateway can interface with many different formats, such as electronic data interchange (EDI) gateways or Health Insurance Portability and Accountability Act of 1996 (HIPAA) translators.

Service Mediators provide a common service contract and service message interface that can be translated to specific vendor offerings. Although three different products may have similar capabilities and a service interface, they may differ slightly. Service Mediators handle those differences.

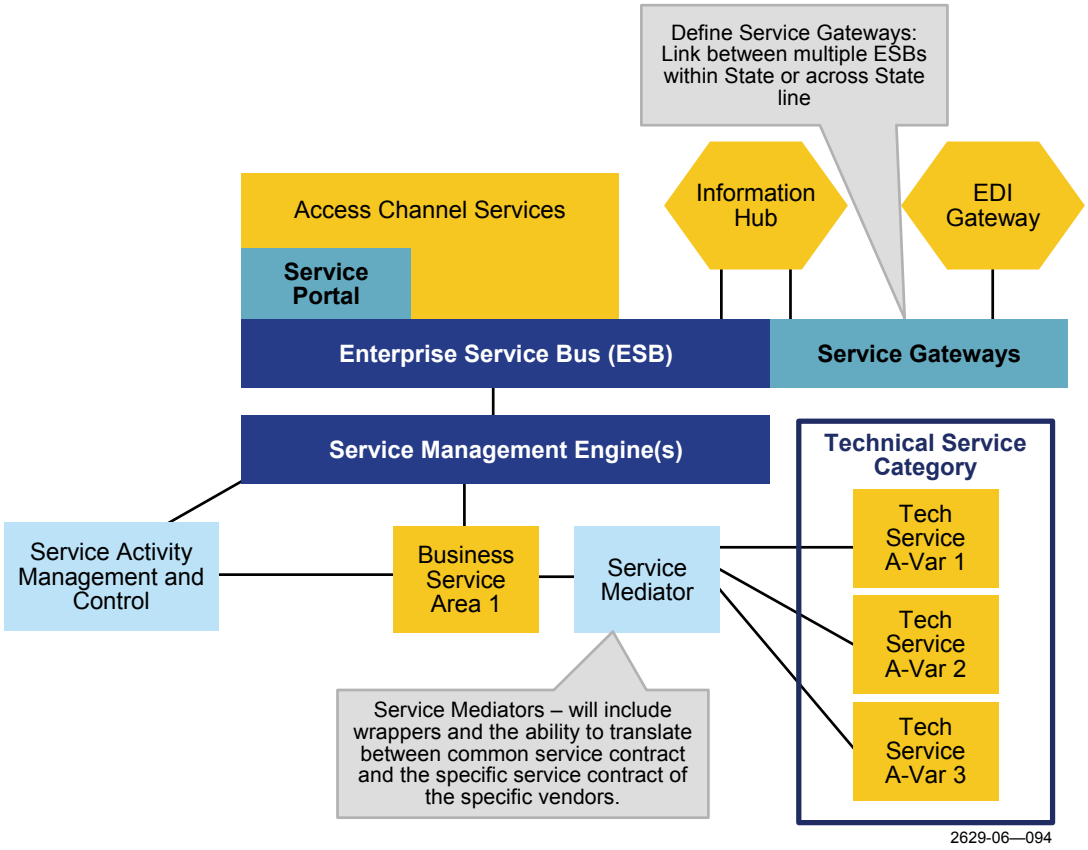



*Figure 7-7. Service Gateways and Mediators*

## Business Services

Part III Chapter 4 discussed MITA business services in detail. Although business services expose the business logic for a particular business process, they must be integrated with the MITA infrastructure to connect with other users and other services.

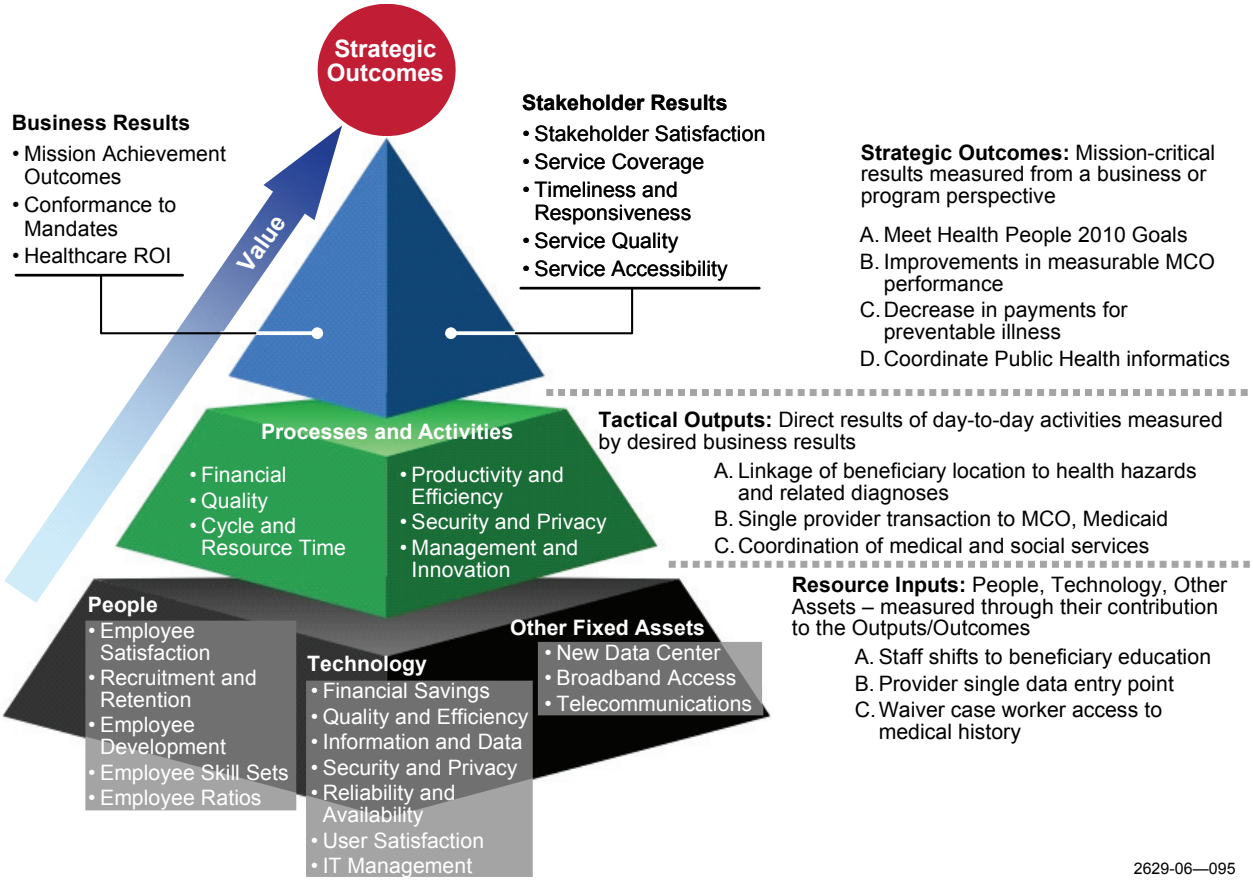
## Technical Services

Part III Chapter 6 discussed MITA technical services in detail. Although technical services expose technical functionality for a specific capability of a technical area, they must be integrated with the MITA infrastructure to connect with other users and other services.

## Performance Management

Performance is often defined from each person's or organization's perspective. To create a common transformation approach, MITA must create a shared definition of business outcomes

and results and a consistent approach to systematically gather information. The Strategic Performance Model shows in graphic format a set of capabilities, including associated integration of data collection, for strategic performance measurement, outcome analysis, and reporting. The Strategic Performance Model, shown in **Figure 7-8,** tailors the Federal Enterprise Architecture (FEA) Performance Model to the healthcare area. The Strategic Performance Model will provide a way to correlate policy changes, program changes, and business process changes. These changes are captured via measures that States can integrate and analyze to assess their impact on Medicaid.




**Measurements are taken at every level: Strategic, Tactical, Resources**

***Figure 7-8. Strategic Performance Model***

The Strategic Performance Model is vital to making a business case for change. MITA has categorized strategic outcomes as Business Results and Stakeholder Results. The Strategic Performance Model has three levels — Business Results and Stakeholder Results (at the top); Processes and Activities (in the middle); and People, Technology, and Other Fixed Assets (at the bottom). The model demonstrates the complex interdependencies of changes at each level.

The **Business Results and Stakeholder Results** level includes the following:

- Business Results consists of three elements — Mission/achievement outcomes, conformance to mandates of Medicaid Federal and State legislation and policy, and a healthcare return-on-investment calculation
- Stakeholder Results, which measures stakeholder satisfaction, identifies the level of service coverage and measures the timeliness and responsiveness of services with service quality and service accessibility

The Strategic Performance Model must use current measurements and must be used as part of the planning and prioritization process.

The measures must be available in reports and forms that States can use to make operational decisions and strategic changes. The results must be consistent with overall healthcare measurements and outcome initiatives, such as Healthy People 2010 and those used by managed care organizations. Performance measures must be adaptable so States can assess the impact of new programs. Two examples are new measures of improvements in illness prevention through early detection programs and measures of the effectiveness of other programs of cross-agency coordination. This level must be supported by a consistent approach to business process and activity modeling and an integrated set of data collection and analysis capabilities.

The **Business Processes and Activities** level measures and analyzes business areas to identify changes that might improve business and stakeholder results. Elements for assessment of future changes in the level include the following:

- Financial measures
- Quality measures
- Cycle and resource time measures
- Productivity and efficiency measures
- S&P measures
- Indicators of management and innovations applied to the area

These measurements will be both quantitative and qualitative and used as part of the business area improvement process. Consistent data is collected with the support of a set of performance measurement utility services and the definition of a shared resource for policy, performance measurement, and support for strategic outcome measurement. Specific performance measurements will be defined in the detailed definition phase with the Strategic Policy and Performance Portfolio.

The **People, Technology, and Other Fixed Assets** level includes three elements:

- People make up the human element model for each business area, which defines the types of roles performed, by whom, when and how they are performed, and with what skills (current skills and those needed in the future). MITA will map the human element to each business area and to the business processes in each area and identify skills that exist today within the State contractor health administration and service industry and those that will be needed in the future. The human aspect of the process is one of the most significant, and any changes will affect the business process and activity level and, in turn, business and stakeholder results. The human element will also include measures of employee satisfaction and States' ability to recruit and retain staff. MITA maps people skills to technologies that States can deploy (e.g., to determine the number of staff a State needs, which will depend on the level of automation and the impact of roles and responsibilities).
- Technology is a critical resource that can affect each business area and program. MITA will define common, shared improvements by introducing utility services or generic architecture elements. These improvements can serve as drivers for higher level business process changes.
- Resources include new capabilities that all business processes can share, such as new networks or a new set of interfaces and data management functions. Resource changes must be linked to the business areas they affect.

The Strategic Policy and Performance Measurement Portfolio will refine the initial set of solutions and create solutions for the strategic policy and performance measurement and related strategic hub architecture. As business cases are developed for individual or shared initiatives, States can use the Strategic Performance Model to compare and prioritize the next changes for investment.

State Medicaid organizations can use the Strategic Performance Model in many ways. Each organization can use, adapt, and extend the core set of measures. As the organization changes, it can introduce additional measures and generate a more complete view of daily operations. These tactical outputs are linked to the Process and Activity level and reflect business process changes made to reach new target levels of achievement. As State providers reach a certain level of achievement for a program and business area, they can address new opportunities for improvement. Their achievements will result from a combination of process changes, new technologies, new skills, and the right kinds of resources.

The Strategic Performance Model and associated measures can be integrated and aggregated and can provide an increasingly more consistent view of business results and the level of stakeholder satisfaction. States can compare policies and programs and can share good and better practices. States can compare strategic outcomes but will need a common shared set of strategic measures collected in a consistent manner.

## Performance Measurement Definition

Performance measurement focuses on creating a strategic policy and performance-driven environment that supports benchmarking outcomes, recognizing performance improvements, and responding to National Health Information Infrastructure (NHII) initiative strategic changes (e.g., public health surveillance). Strategic policy and performance measurement capabilities and the related strategic hub, strategic data model, performance utility services, and connection to data sharing and coordination elements are all part of an integrating strategic policy and performance throughout MITA.

## Key Performance Measurement Concepts

Performance Measurement will develop and publish common measurement criteria that link to and extend Strategic Performance Models. It will also refine and specify performance measurement utilities that will define a standard method of data collection across MITA organizations. MITA will develop standard report formats and utilities for performance measurement, key elements of which include the following:

- Identifying the kinds of data needed for strategic decision making and a set of basic strategic analysis scenarios
- Establishing consistent measurement definitions and guidelines for adapting and extending those definitions. Those guidelines will map to national and healthcare industry measurement definitions as much as possible. For example:
  - Defining strategic outcome processes, templates, and reports to support normative analyses and comparative analyses between States and programs
  - Using normative analyses to compare a State's performance with "the norm," based on performance measures collected over multiple organizations or populations
  - Using comparative analysis to compare a State's performance with past performances or to that of other organizations
- Adapting and extending the MITA Strategic Performance Model from the FEA Performance Reference Model

## Additional Performance Measurement Detail

- Performance can be measured independent of the type of system, even if Medicaid functions are outsourced.
- Gathering performance metrics generally requires that metrics be collected at diverse data collection points and aggregated into composite reports.
- Performance utilities will enforce performance measurement consistency.
- Tools for standard reporting and for ad hoc special purpose needs will reinforce the benefits of consistent performance measurement and support normative and comparative analysis.

### Performance Measurement Challenges

State Medicaid organizations' strategic functions and policies have often been ad hoc and with limited support. Agencies have common problems and common data needs and can and should view policy performance measurement outcomes as more than one-time events. MITA will integrate them into MITA processes to allow States to define them better and provide meaningful comparisons. MITA will also translate concepts of policy management, performance measurements, and the technologies for data analysis and reporting to make them useful to support Federal and State policy needs. The data and reports must be protected and secure.

## Service Interoperability

Interoperability is one of the key MITA goals. Currently, many States address interoperability in some manner, whether through a HIPAA translator or by trying to connect with other agencies in the State or with Federal agencies.

MITA interoperability services are part of the overall answer, but business challenges exist as well. Technical challenges are addressed here, but we also recognize the need to address business interoperability challenges, which include the following:

- Lack of incentives for States to cooperate will require "selling" State organizations on the benefits of interoperability.
- Lack of funds for cross-organization activities may require changes to budget allocations.
- Lack of infrastructure to support interoperability and reconciliation will slow implementation.
- Legacy systems with disparate definitions and stovepipe systems might not conform to new standards for interoperability.

The services-oriented interoperability approach described here provides technical enablers that will overcome obstacles and provide common ground for addressing key issues, which will reduce the learning curve and allow the MITA community to share the architecture and design experience. States can apply MITA hub architecture, interoperability and access channels, and utility services based on standards-based contracts to meet these challenges, but the focus is on creating a service-oriented government approach, as shown in **Figure 7-9.**

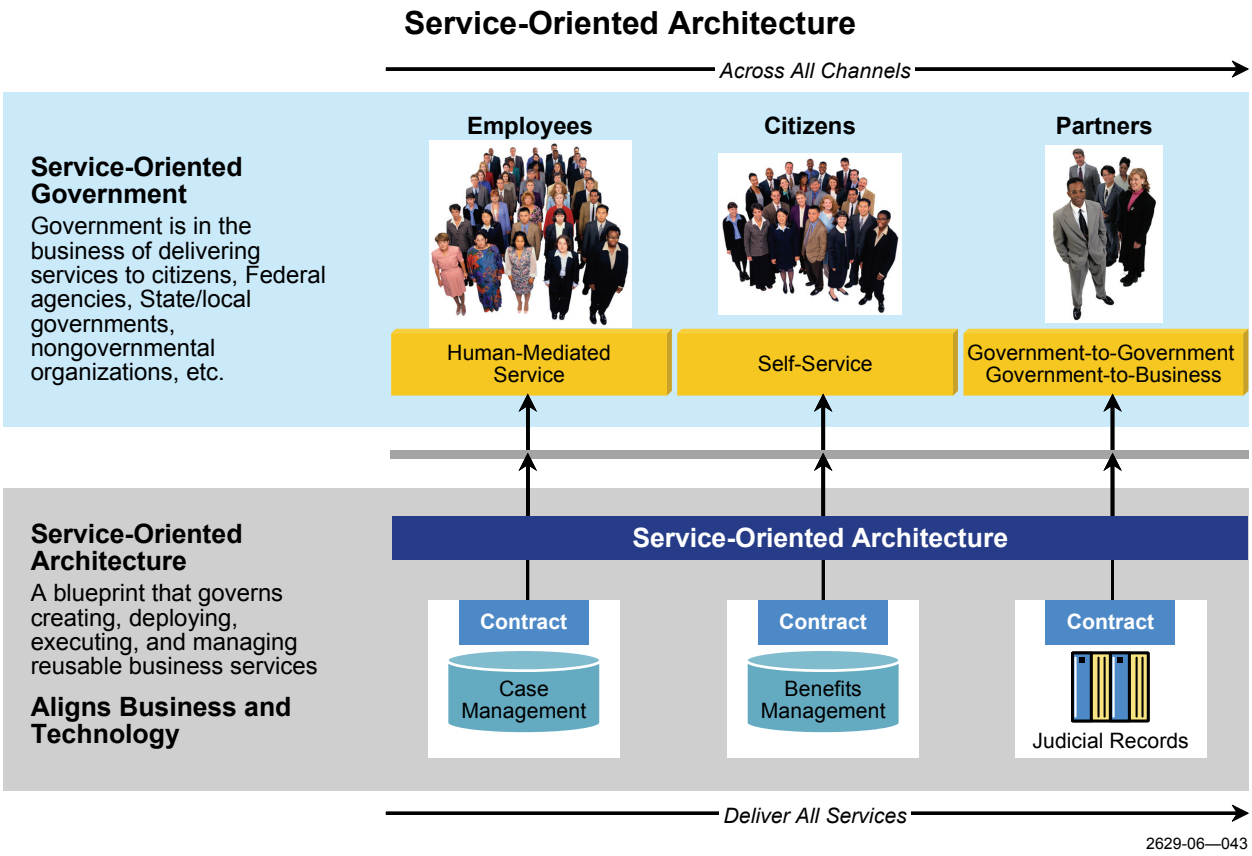



*Figure 7-9. Service-Oriented Architecture*

## Key Service Interoperability Elements

The key concepts for service interoperability are as follows:

- Use services and messaging standards for real-time, business area-to-business area, and cross-organizational communication.
- Use services to define clear processes and consistent mechanisms for system-to-system communication, with the definition of communication requirements, and recommend technologies for automated responses (e.g., WS and XML protocols).
- Use services to define a common MITA interface that reduces complexity and shields States and their partners from technical details.
- Use services to define common functions and features that States can separate from applications and implement using service utilities.
- Use services to define a logical interoperability architecture (a "service overlay") based on hub technology and communication protocols that States can adapt, based on channel definitions and virtual communication access mechanisms.

- Support alternative access to the same information and services, including Web (human interface), Internet (machine to machine), and others. Data, processes, and services can be hidden behind interoperability channels that can adapt to meet changing needs using configuration files.
- Use a business-oriented service interoperability process that focuses on the business-needs perspective, based on three principles:
  - Define common semantics (the meaning of, for example, a message)
  - Define common syntax (the structure of, for example, a message)
  - Define a common mechanism (a means of exchanging information)
- Define a set of common service elements that States can adapt through variants and extensions. MITA's goal is to define what is common and build it for change ("design for change") but also provide limited change management within the service layer through adaptable "wrappers."
- Define service interoperability solutions that rely on common definitions for channels and utilities that are specific to business areas but are designed with common underlying architecture and common utility components.
- Define and create virtual access mechanisms that hubs or individual State systems can use to exchange information.

## Additional Interoperability Detail

Hub architecture is a key concept for interoperability services. Hub architecture differs from data marts and data warehouses in that it does not remove data to a central site. Virtual hubs collect data on demand from multiple locations, but each organization retains control and ownership of its data. By providing access and data definition information to hubs, States and other partners can host common access channels, interoperability channels, and utility services that let hubs extract data and direct queries to other hubs.

The Logical Interoperability Model for a hub architecture shows three types of hubs:

- Tactical hubs, which collect information around a specific business area. For example, Medicare, Medicaid, and public health organizations might have tactical hubs that manage data, member information, and the necessary utilities to collect information about them.
- Strategic hubs, which collect summary information from multiple disciplines. A strategic hub might collect diagnosis information from Medicaid and Medicare systems and disease information from public health organizations and compare the two.
- Data-sharing coordination hubs, which store data-sharing agreements and broker the exchange of information among organizations.

## Service Interoperability Models

### Key Elements of the Access Channel Model

The Access Channel Model performs several key functions:

- Access channels allow State Medicaid staff to access data and information by multiple means (e.g., mobile, wireless, PDAs, and kiosks) and to interface with organizations that provide batch interaction with messages. Private–Public Partnership Access might include an organization that is allowed access by contract. The features and functions accessed must be clearly defined.
- Access channels protect rights to certain information and allow information sharing through specific interoperability channels. These exchanges can be planned for and collaborative tools provided. The access channels and interoperability channels will include defined connectors. Connectors will define alternate access approaches. Access approaches will be adaptable based on policy or failure or recovery conditions.

**Table 7-1** answers questions about the Access Channel Model.

*Table 7-1. The Access Channel Model*

| Question | Answer |
|---|---|
| Why is the Access Channel Model important to MITA? | The Access Channel Model shows multiple access channels supported by utility services. Easy data access will transform the Medicaid business. The key concept is the importance of separating access channels from interoperability channels. |
| Who should understand the Access Channel Model? | Designers and implementers of systems should evaluate possible access channels and interoperability channels to make data as readily available as possible. |
| How will the Access Channel Model be used? | System designers and implementers should adopt an architecture that separates access channels from interoperability channels and uses common utility services to simplify development. These utilities may be nationally shared or shared within a State or among certain Medicaid systems. |
| How will the Access Channel Model be refined and updated? | The Interoperability Portfolio will update the Access Channel Model. Detailed interoperability guidelines and standards will be selected or defined. |
| How will the Access Channel Model support ongoing business decision making? | New IT procurements should adopt the concepts of isolating access and interoperability through the use of utility services |

### MITA Interoperability Model

MITA has taken a strategic business and technical approach to interoperability, as shown in **Figure 7-10**. MITA views interoperability as subfunctions, topics, and types of communication, and it understands that conflicts can occur and common solution patterns can be used.

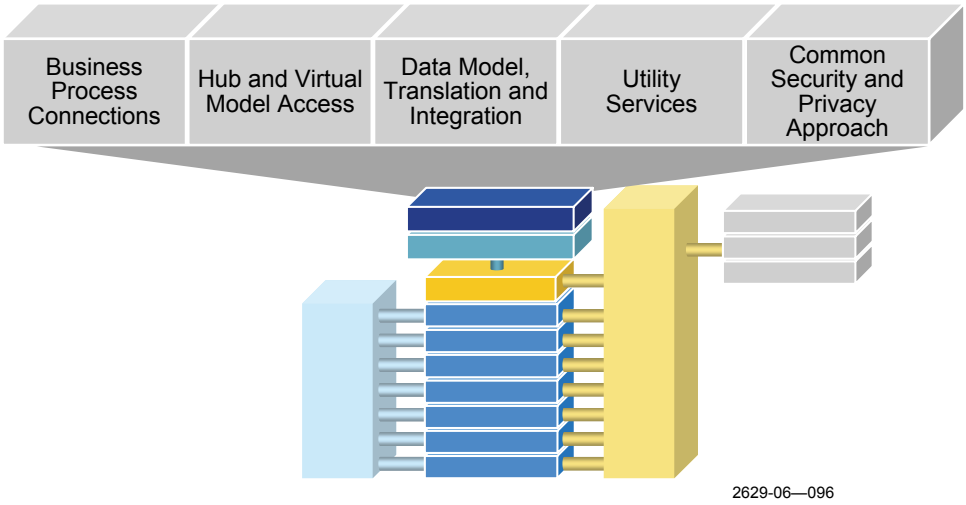



*Figure 7-10. Conceptual Interoperability Model*

MITA will define separate interoperability channels for each type of information flow and give States a definition of utility services that they can share across the Medicaid enterprise.

MITA will refine interoperability channels collaboratively through the portfolio process.

### Key Concepts of the Interoperability Model

Key concepts of the Interoperability Model include the following:

- **Interoperability**. The model uses common elements and approaches that fit with those of other models and that States can adapt to meeting their changing needs.
- **Connectors**. Each business area includes business processes and connectors. Connectors are defined by the type of connection — asynchronous communication, publish-and-subscribe, and request-and-respond — and by the type of information or services exchanged. Topics, subjects, or access to a given type of information are grouped on a common logical channel. S&P access control may also require separate channels.
- **Hub and virtual model access**. Transmitting and receiving services and information over an interoperability channel can take many forms. A hub architecture is the most mature and offers additional S&P control points, which can locate utility services on the hub. After the request is at the hub, the utility services can access information and services through virtual model access.
- **Data model and integration**. Interoperability channels can define data translation capabilities in ways that mask incompatibilities.
- **Utility services**. Utility services and common utility elements create an interoperability channel. An interoperability table defines these elements and allows for adaptations.

- **S&P service components and utilities**. S&P service components and utilities will be defined with alternative levels of protection, depending on the services and topics communicated over the channel.
- **Interoperability conflicts**. The model identifies interoperability conflicts through interoperability assessments, which it groups into business-centric pieces (based on common business interests or purposes) and defines by interoperability channels.
- **Functionality**. The model provides functionality through individualized utility services (i.e., they are not built into each application).

## Logical Interoperability Level

MITA will implement its interoperability concepts through a configuration shown in **Figure 7-11,** which uses hubs, virtual private network capabilities, and a common set of utility services to create the logical model and address interoperability at many levels. The Logical Interoperability Model can address a minimal set of information sharing needs in a standard way for intra-State data sharing (with other State departments), between business areas (storing the data in strategic, tactical data hubs), and with partners (through the data sharing and coordination hub). The model and concepts can be extended based on workload and on recovery and contingency planning needs.

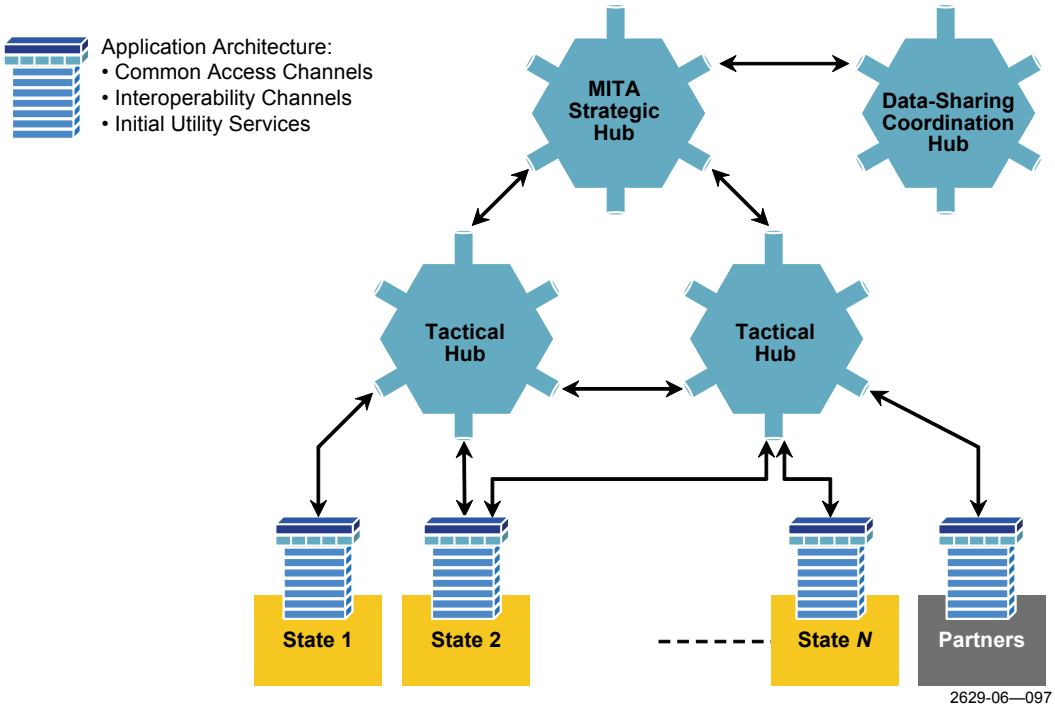



*Figure 7-11. Logical Interoperability Model*

Figure 7-11 shows hub interconnection and shows how utility services and the interoperability definition (configuration files) and security utilities fit together. Its chief characteristics are as follows:

- Virtual hubs provide access to data owned and stored by individual States and other organizations.
- Common access channels, interoperability channels, and utility services assist data sharing and coordination.
- Partners and States (shown as States 1 – *N*) will use a common format. Each State and partner will include utility services and interoperability services functions.
- The three types of hubs are strategic hubs, tactical hubs, and hubs used for infrequent data sharing and coordination. Regular partners that have tactically useful information, such as the Centers for Medicare & Medicaid Services (CMS) or other benefits programs, may be hooked to the tactical hub.
  - *MITA Strategic Hub.* This hub deals with strategic policy and performance measurement capabilities. Performance and analysis data will be collected and shipped on an event or periodic basis and stored in a data mart configuration with additional related information.
  - *Tactical Hubs.* Two or more tactical hubs will support functions that cross State lines or, in cases where data is common, including master reference information that MITA will update and share with all States to assure consistency.
  - *Data Sharing Coordination Hub.* This hub will gather and disseminate data based on agreements between partnering organizations. It will also link to elements with the National Health Information Infrastructure (NHII) and other partners, such as the Bureau of the Census or the National Committee on Vital and Health Statistics (NCVHS).
- **Application Architecture**. The AA links between a business area and common interoperability utilities and between common service utilities and interoperability service functions driven by the interoperability table(s) at each State and hub. A consistent method of updating these interoperability channels is discussed later in this chapter (under “adaptability and flexibility”).

## Logical Hub Architecture

MITA hubs are built on standard hub architecture, as shown in Figure 7-11 above, and can be configured to address tactical, strategic, and data-sharing and coordination functions. The hub architecture consists of three layers:

- **Interface management layer**. The interface management layer is the core. It receives messages based on defined interoperability channels; handles all the message buffering, transport protocols, and any message translation needed; includes any routing to the data management or the utility services layer; and supports the adaptability needs or any necessary manual functions, such as special queries.

- **Data management layer**. The data management layer can house data stores that are either data marts or more relational data models. It also includes a virtual data access capability.
- **Utility services layer**. The utility services layer represents the portions of utility services that reside on the hub or server (often called the *servlet*) and can provide capabilities run on the hub, such as access to virtual models, collection, filtering, and delivery of blocks of information to the business area.

**Table 7-2** answers questions about the Interoperability model.

### *Table 7-2. The Interoperability Model*

| Question | Answer |
|---|---|
| Why is the Interoperability Model important to MITA? | The Interoperability Model describes the business capabilities and technical functionality necessary to achieve efficient system-to-system interactions within Medicaid programs and between Medicaid and other MITA initiatives. |
| Who should understand the Interoperability Model? | Designers and implementers should understand the concepts in the Interoperability Model and incorporate them into system designs. |
| How will the Interoperability Model be used? | The Interoperability Model will provide guidance and recommendations that support the development and implementation of services and data that the MITA community can share, although States will retain their autonomy. States can follow the model to achieve cross-organizational information sharing through a common approach. |
| How will the Interoperability Model be refined and updated? | The Interoperability Portfolio will update the Interoperability Model. The next steps will be development of detailed interoperability specifications. |
| How will the Interoperability Model support ongoing business decision making? | New IT procurements should adopt these concepts of MITA interoperability. |

Initial designs for tactical and strategic hubs, summarized in **Table 7-3** and **Table 7-4**, will be developed and enhanced by the MITA team in the future. Both will feature a three-level architecture. The tactical hub shows the processing of tactical data in a data store, available through virtual access or interfaces.

The strategic hub architecture provides analytical services for policy, performance measurement, strategic studies, and exchanges among health policy makers.

## *Leveraging Interoperability Projects*

- Intelligence agencies have an extensive "infostructure" program that links more than 20 business areas.
- These projects address Federal-to-State communications, such as communications that involve the Environmental Protection Agency (EPA), the Department of Justice (DOJ)

(e.g., on criminal investigations), and communications concerning State grants with the Global Justice Network initiative and its definition of standard XML-based schemas.

- Interoperability and cross-boundary issues are an active area of architecture alignment that the Federal Chief Information Officers Council is pursuing with the Office of Management and Budget's FEA-PMO, the architecture team from the National Association of State Chief Information Officers (NASCIO), and with industry associations that support both Federal and the State initiatives.

## Candidate Future Interoperability Activities

### Table 7-3. Description of Candidate Future Interoperability Activities

| Activities | Description |
|---|---|
| Refine Interoperability Models by defining interoperability channels | Define specific interoperability channels for the business and technical levels, giving attention to both healthcare protocol calls and transport, service, and message protocols. |
| Define Interoperability Standards (Reference Table 7-4, Sample Interoperability Channel Definition) | Identify initially preferred standards and other standards that can be used in the format displayed in Table 7-4. |
| Interface Specification Project | Define business area interfaces and create interface specifications. |
| Logical Hub Definition and Development Project | Create a sample hub for a specific purpose and with limited participation and use it as a generic design for hub configurations. |
| Message Exchange Formats Project | Define external initiative message exchange formats. |
| Define and Develop Interoperability Utility Services | Define in greater detail the utility services and related interoperability channels needed for interoperability. Develop a basic set of interoperable utility services and connect to the related S&P utility services and those involved with adaptation and flexibility. |
| Hub Development Project(s) | Select a business problem for interoperability, both as an external initiative and as an internal business improvement. The series of tactical, strategic, and data coordination hubs will be developed. |

### Table 7-4. Sample Interoperability Channel Definition

| Interoperability Channel (examples) | Identifier | Utility Service | Integration Type (examples) | Standard (examples) | Maturity | Action |
|---|---|---|---|---|---|---|
| ■ Receive data from providers<br>■ Receive information from vital statistics | Utility service name | Specify types of utility services | ■ Event<br>■ Message<br>■ Message-and-attachment<br>■ Request-and-response<br>■ Publish-and-subscribe | ■ HIPAA<br>■ Subset of HL7<br>■ SNOMED | ■ Released (products on the market)<br>■ Product commitment<br>■ Waiting for balloting<br>■ Proprietary product<br>■ Define ourselves | Link to portfolio project or activities |

## Security and Privacy

The MITA S&P approach leverages government, industry, and federally funded academic research on security, privacy, and continuity of operations, with a strong link to available and emerging products and solutions. Others have tried to create a separate S&P architecture and set of products. We treat S&P as a crosscutting design aspect that includes a limited group of common centralized elements but that may have many mechanisms and controls that are distributed.

### Terminology and Concepts

This section provides some background on S&P terms and concepts.

- **Authorization** — Authorization (which addresses the question "What can you do?") governs the resources and operations that the authenticated client can access. Resources include files, databases, tables, and rows, as well as enterprise-level and MITA-level resources (e.g., registry key and configuration data). Operations include performing transactions such as enrolling a beneficiary, transferring a beneficiary from one provider account to another, or prior approval (also called *prior authorization*).
- **Auditing** — Effective auditing and logging is the key to nonrepudiation. Nonrepudiation means that a user cannot unreasonably refuse to perform an operation or initiate a required transaction the user has agreed to. In an e-commerce system, for example, nonrepudiation mechanisms ensure that a consumer cannot deny ordering 100 copies of a particular book if the consumer in fact ordered them. A MITA variation might be refusing to perform a surgery after the audit trail shows that the provider approved it.
- **Confidentiality** — Confidentiality (or privacy) means ensuring that data remains private and confidential and that unauthorized users (or eavesdroppers who might monitor traffic across a network) cannot view it. Common methods of ensuring confidentiality include encryption and access control lists (ACLs), through which

personal medical information is specifically handled in such a way as to follow certain privacy procedures, as discussed in greater detail below.

- **Integrity** — Integrity is a guarantee that data is protected from accidental or deliberate (malicious) modification. Like privacy, integrity is a key concern, particularly for data that passes across networks. Integrity for data in transit (often called "data in motion") typically uses hashing techniques and message authentication codes to detect inconsistencies and require retransmission.
- **Availability** — Availability means that the system will remain available to legitimate users. (Some attackers, such as those who have been denied service, may seek to crash an application or overwhelm it so other users cannot access it.)
- **Asset** — An asset is a resource of value, such as data in a database or a system resource.
- **Threat** — A threat is a potential occurrence (malicious or otherwise) that might harm an asset.
- **Vulnerability** — Vulnerability is a weakness that makes a threat possible.
- **Attack (or Exploit)** — An attack is an action taken to harm an asset.
- **Countermeasure** — A countermeasure is a safeguard that addresses a threat and mitigates risk.

## MITA Security and Privacy Focuses

**Requiring Integration from the Beginning.** MITA's S&P features must be integrated throughout MITA, including with legislative and policy goals, and supported with a risk management approach. The discovery of the S&P business needs is often a neglected activity. Some organizations have attempted to "bolt on" S&P features, which is both difficult and problematic, as experience with HIPAA has shown.

**Taking into Account the Business Perspective.** S&P is too important an issue for merely the technical specialist. It must also include a business perspective. MITA seeks to bring S&P issues to the attention of all involved with the Medicaid Support System, weave S&P considerations into all aspects of the business process, and incorporate each new business initiative and each change in technology. Although S&P is complex, it must be understood by management, business leaders, and partners and customers of the services delivered, taking into account their differing levels of understanding and differing needs. Citizens who receive services and supply personal information must trust Medicaid's ability to secure and protect their information. Organization leaders must protect the valued assets and maintain continuity of service.

MITA must consider the business impact of a threat or attack from outsiders or insiders, based on the particular business process and organizational dependencies. There are many common, known threats or challenges for S&P that MITA will leverage in its S&P business impact analysis. The business modeling approach uses business-use cases. To integrate S&P into business models, MITA must extend business-use cases with S&P-specific information.

**Candidate S&P Use Cases.** Candidate S&P use cases include:

- Peer identification and authentication — man in the middle, principal spoofing
- Data identification and authentication — forged claims
- Data integrity — unintended and unauthorized viewers
- Transport data integrity — message alteration, replay of message parts
- Single Object Access Protocol (SOAP) message integrity — attachment alteration
- Data confidentiality
- Transport data confidentiality
- SOAP message confidentiality
- Message uniqueness

Other security scenarios include:

- Denial of service
- Virus
- Worm
- Defacing of Web site or portal
- Insider attack
- Insider "watching own actions" — Hansen watching the watchers

Additional privacy scenarios include:

- Inadvertent release and correction — statistical analysis did not hide personal information
- Violation of usage agreement — passing information to others
- Unauthorized access to specific personal information identified information — pattern of access not consistent with role
- Health crisis override of privacy preferences — "the next SARS"

S&P mechanisms must be integrated into the business and technical models. S&P activities are crosscutting activities that must define protection mechanisms, components, operations processes, and roles and responsibilities. It is a business principle that S&P is a factor in all services and models.

**Providing Protection with Low Maintenance.** MITA seeks to create a protected and trusted environment that is economical to maintain, by seeking a balance between addressing weaknesses found in an S&P assessment and making needed changes from a strategic point of view.

**Consistent Across Medicaid.** MITA will provide a consistent base for the Medicaid community and align with initiatives such as the FHA and the NHII as they address S&P. MITA must also address common issues as seen from other industries.

MITA's consistent approach will allow agencies to react "as a community," using common terminology, addressing common threats, sharing concerns, and detecting, deterring, and responding to common issues that might affect Medicaid and the healthcare industry.

**Adaptable/Responsive.** S&P standards change frequently in response to new threats and viruses and to the new technologies that counter them. MITA must adapt and extend S&P features as new threats and new forms of attack are identified.

**Platform/Software Independent.** MITA S&P services and solution sets are designed to meet key principles, which transcend implementation technology and application scenarios. S&P models must simultaneously meet policy needs using the best available technologies within the resources. Fortunately, the S&P field is very active and many products and standards are evolving.

Some models are largely common sense, but have been specifically defined and proven mathematically in many cases and used by many vendors in their products. How they are implemented may vary, and in some cases the vendors have created their own marketing name for the same concepts. Two vendors might develop the model with a different architecture, such as Oracle Security versus the plug in for DB2, an approach used by Protegrity. Both vendors are using essentially the same decentralized labeling approach but the products differ in some respects.

The MITA model can be used in different architectures. For example, the user could pull roles and responsibilities from a registry, or the server could pull them from a directory such as Lightweight Directory Access Protocol (LDAP), but both approaches would be performing RBAC. The mechanisms might also differ, one using a certification approach and other using an approach, such as a "security ticket," and in some cases allowing users to take either approach. Within the MITA community many choices will be common, but MITA can adapt to others by providing hooks for extensions. Currently the RBAC and decentralized label models (DLMs) are two critical elements to be leveraged. (The Multi-Level Security Model, Federated-Identification Model will also be considered.)

**Cross-Agency Integrated and Aligned.** MITA integrates S&P in the enterprise, aligning it across the enterprise with a set of controlled and managed interfaces that follow a set of policies. S&P risks must reflect decisions made jointly by Federal and State policy management. This goes beyond the traditional boundaries of the Medicaid Management Information System (MMIS) by including partner agencies in human service benefits delivery, such as State IT delivery, the provider community, and beneficiaries/members/citizens themselves.

S&P services define standard S&P mechanisms to facilitate the exchange of information among multiple organizations. The portfolio will address both policy and technical issues regarding secure data exchange. MITA will address additional threats and challenges as it develops

solution sets, including by selecting and refining other models and more specific mechanisms and architecture patterns.

The MITA team is studying security models for collaborative environments. This area has been refined with the help of services research and based on experience with other federated communities that must collaborate. These security models could be very valuable within the areas of strategic planning, performance tracking, and disease management on collaborative projects to improve healthcare management.

S&P services will define an S&P framework that focuses on a common toolkit approach to protecting interoperability and information sharing. Toolkits will include sample security agreements, security policies, and technical recommendations and utilities that do the following:

- Provide consistent and integrated S&P through integrated S&P utility services and interoperability channels.
- Use mature and emerging S&P standards.
- Provide multiple levels of security that States can adapt to meet changing and varying needs.

**Going Beyond HIPAA.** S&P goals are guided by HIPAA, but most go beyond HIPAA to provide an S&P solution set that States can adapt and extend. MITA will put in place specific S&P mechanisms to achieve its interoperability and data management goals. S&P is already a strong focus with HIPAA and will become stronger with MITA.

**Defining Goals and Objectives by Formal and Informal Policies.** MITA bases its formal policies on industry-standard S&P language that States can access and share, with security service elements in packages and in a unified but distributed and federated S&P framework.

## Basic Approach

MITA has tied S&P to the architecture in State Medicaid enterprises and, to some extent, within some cross-government activities. MITA has done this in parallel with the efforts of Federal and State CIOs, participants from the National Institute of Standards and Technology (NIST), and other industry associations. MITA has attempted to do the following:

- Explain the drivers for S&P — HIPAA S&P rules that States understand and are actively working on.
- Leverage the activity of upgrading NIST guidance based on E-Government 2002 directives.
- Develop a risk and value management approach that combines experience with Federal Information Security Management Act (FISMA) reporting activities and the Performance Reference Mode.
- Define an approach that balances short-term reaction (which often occurs with a new virus or security breach) with longer term activities to integrate S&P.

- Define a process to build services and solution mechanisms into all portions of the architecture and link them to standards and commercial products.
- Leverage the work with the FEA Reference Model — S&P Profile Phase I and participate in developing Phase II S&P solutions and mechanisms, tying them to the NASCIO Security Guidance and to closely related NIST HIPAA Security Guidance and initiatives of the healthcare industry and of other industries (such as insurance) to adopt and influence S&P standards.
- Other documents used for background and reference are:
  - NIST documents
  - HIPAA S&P rules
  - CMS reports
  - Department of Health and Human Services (DHHS) guidances
  - NASCIO guidances

### *Table 7-5. Basic MITA S&P Principles*

| Principle | Concepts |
|---|---|
| Compartmentalize | Reduce the surface area of attack. Ask how you will contain a problem. If an attacker takes over your application, what resources can the attacker access? Can an attacker access network resources? How are you restricting potential damage (e.g., firewalls, least privileged accounts, and least privileged code are examples of compartmentalizing)? |
| Use least privilege | Run processes using accounts with minimal privileges and access rights and thereby reduce an attacker's capabilities significantly if the attacker manages to compromise security and run code. |
| Apply defense in depth | Use multiple gatekeepers to keep attackers at bay. Defense in depth means that you do not rely on a single layer of security and assume that one of your layers may be bypassed or compromised. Can you survive if one firewall between different zones is not operational? |
| Do not trust user input | Your application's user input is the attacker's primary weapon when targeting your application. Assume all input is malicious until proven otherwise and apply an in-depth strategy to validate input, taking particular care to ensure that input is validated whenever a trust boundary in your application is crossed. |
| Check at the gate | Authenticate and authorize callers early — at the first gate. |
| Fail securely | If a system component or application fails, do not leave sensitive data accessible. Return friendly error messages to users that do not expose internal system details. Do not include details that might help an attacker exploit vulnerabilities in your application. |
| Secure the weakest link | Is there a vulnerability at the network layer that an attacker can exploit? What about other points? |

| Principle | Concepts |
|---|---|
| Create secure defaults | Is the default account set up with least privilege? Is the default account disabled by default and then explicitly enabled when required? Does the configuration use a password in plain text? When an error occurs, does sensitive information leak back to the client in a way that the client can use against the system? |
| Reduce your attack surface | If you do not use it, disable it. Reduce the surface area of attack by disabling or removing unused services, protocols, and functionality. Does your server need all those services and ports? Does your application need all these features? |

## Concept Maps

MITA will use the concept map as a navigation tool for the many tools, standards, models, and actions States must take to integrate S&P into all the elements of their enterprises, with special focus on the cross-enterprise data sharing and shared services MITA will define. Figures 7-12, 7-13, and 7-14 presented below are concept maps.

## Basic Principles

Enterprise architecture and S&P architecture must be aligned, as must with changes necessary to "harden" and strengthen the protections, as shown in **Figure 7-12.**

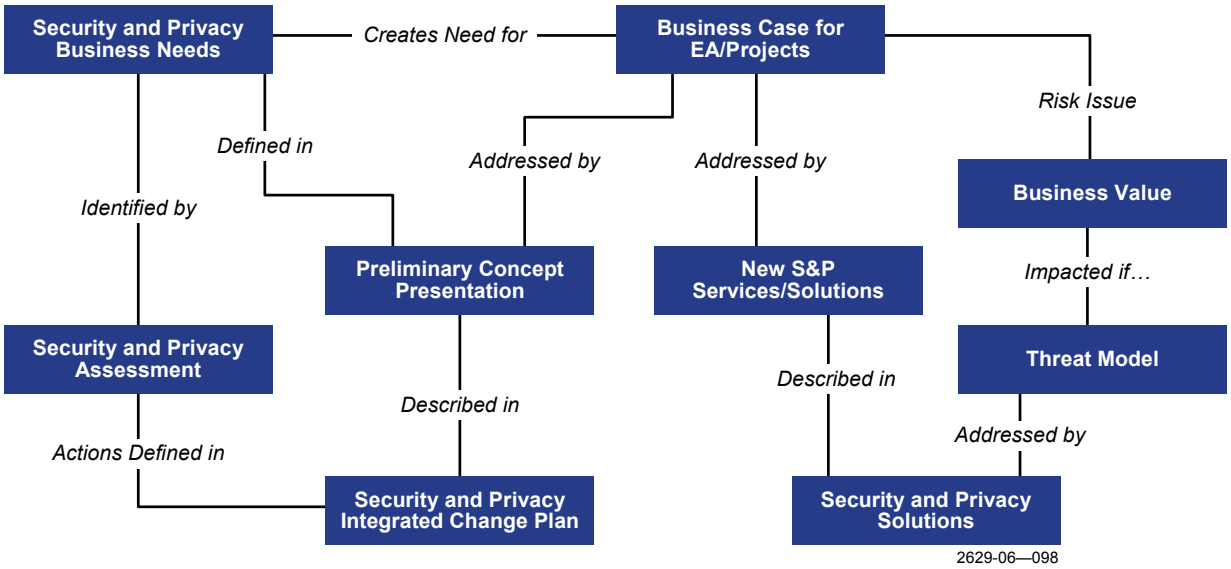



*Figure 7-12. Aligning S&P and Enterprise Architecture*

## Integrate Security and Privacy into Enterprise Architecture

The second concept map shows the steps needed to integrate S&P into the strategy and enterprise architecture and into other related solution sets, as shown in **Figure 7-13**.

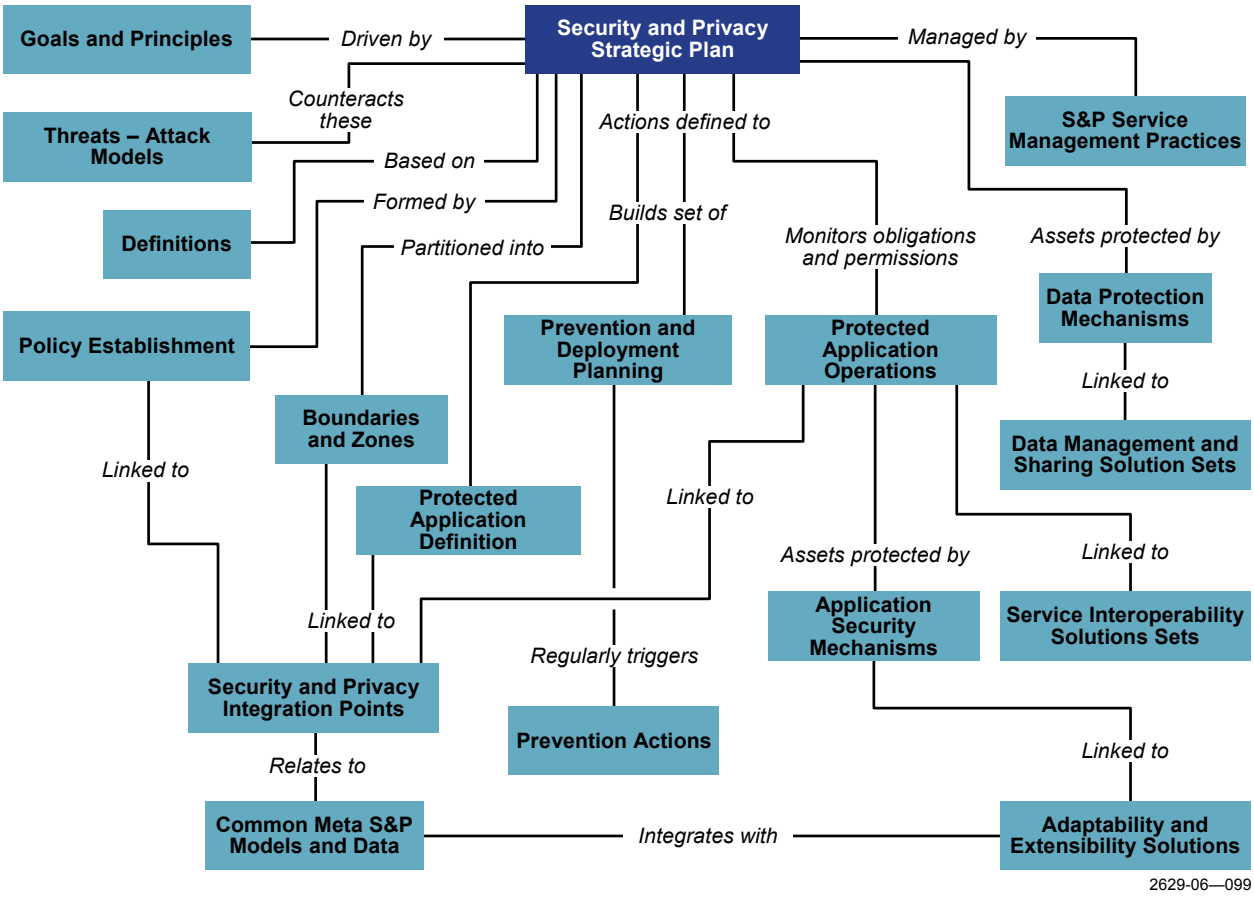



*Figure 7-13. Aligning S&P and Strategy Architecture*

## Security and Privacy Elements

S&P elements and their links are described in the third concept map, shown in **Figure 7-14**.

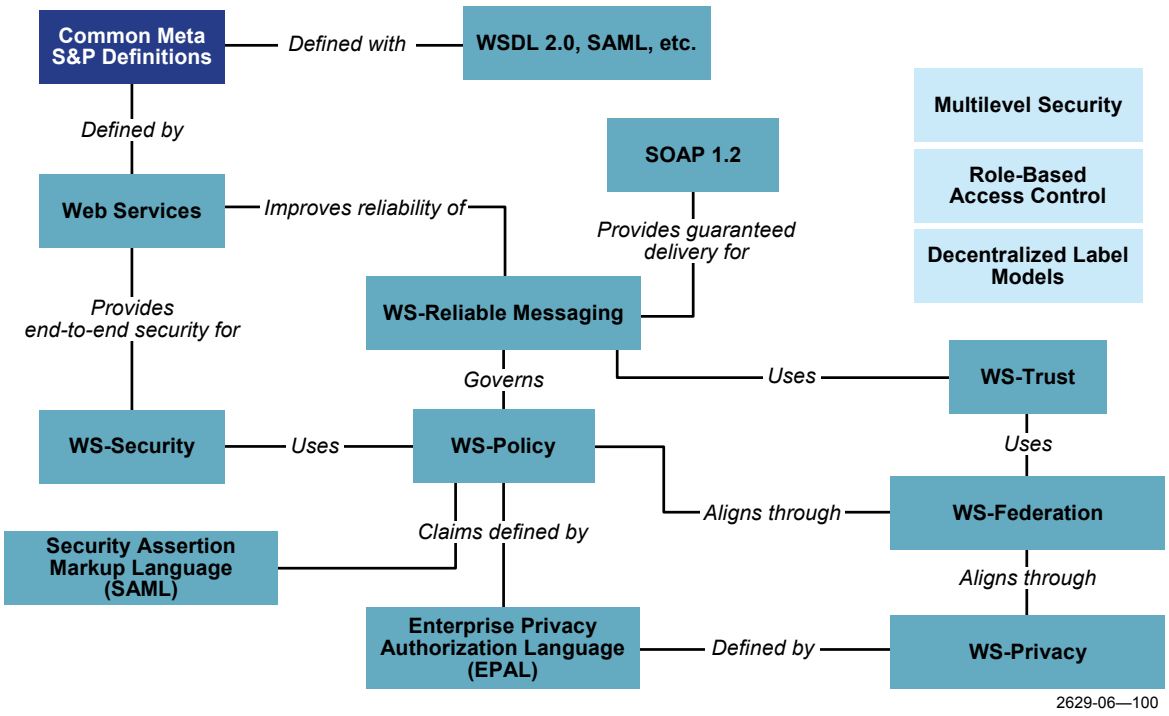



*Figure 7-14. MITA S&P Standards*

## Objective, Model, Architecture, and Mechanism Framework

MITA has defined a crosscutting extended enterprise and layered approach and mapped it to S&P standards with known gaps. The framework, shown in **Figure 7-15**, is based on the Objective, Model, Architecture, and Mechanism (OM-AM) Framework developed by Park and Sandhu from George Mason University.

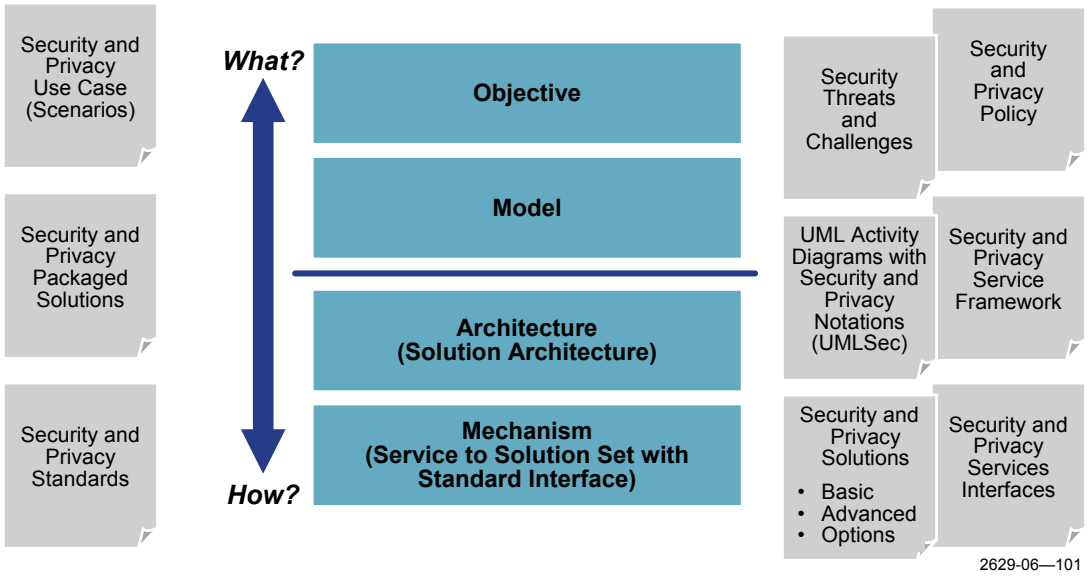



*Figure 7-15. S&P and the OM-AM Model*

Objective and model layers articulate the security objectives. Architecture and mechanisms describe how to achieve them. Within the OM-AM Framework, each layer can map to the adjacent layers in many ways. For example, an RBAC model is very popular (as is a DCM) but different products would implement it in different ways. For example, the RBAC model provides a well-understood way of discussing roles and responsibilities and mapping them to processes to ensure that the same person can both authorize and receive payment. The DCM can be used to define how to label and manage data and documents and how to control access to those documents.

MITA plans to develop additional concept maps and link them to solution sets, standards templates, and the S&P Key Objectives to Threats Concept Map.

## Tools

The MITA S&P Solution Set provides guidance on how to integrate S&P into the business process. The MITA team developed the S&P solution set to create a decision framework that not only balances risk and value, but provides a comprehensive and open approach that responds to evolving threats and complex technologies. MITA developed the solution set using common S&P scenarios. The scenarios are related to MMIS with a business impact- and risk-gathering activity. Elements were derived from the HIPAA S&P rules (relying on the NIST).

## Forms

MITA will develop a set of templates or forms that States can use when defining their S&P approaches. Over time, we expect that these forms and elements will be updated, refined, and expanded. They are related to each other and designed to foster architecture and design reuse. (A

prototype of these forms is under consideration for sharing with Federal and early adopter States and is included in a Design Center Repository.)

## Security Threat Models (aka Attack Models) and Challenges

The MITA team looks at threats from the perspective of their impact on the delivery of services along a channel and the breaking of the service-value chain. Each business area might have one or more service value chains that have goals. One can describe threats based on the purpose of the attack. Each service analysis will include defining the use and the types of services provided by one or more endpoint resources along the defined channel. The threat model was begun with the Threat Modeling approach used by Microsoft and has expanded with specific threats from the HIPAA and health information privacy literature.

The MITA team will organize threat categories around the Spoofing/Tampering/Repudiation/ Information (disclosure)/Denial (of service)/Elevation (of privilege) (STRIDE) acronym used by Microsoft and the associated free analysis tool:

- **Spoofing**. Spoofing is attempting to gain access to a system by using a false identity. This can be accomplished using stolen user credentials or a false IP address. After the attacker has gained access as a user or host, the attacker might attempt further efforts.
- **Tampering**. Tampering is unauthorized modification of data (e.g., as it flows over a network between two computers).
- **Repudiation**. Repudiation is the ability of users (legitimate or otherwise) to deny that they performed a specific action or transaction. Without adequate auditing, repudiation attacks are difficult to prove.
- **Information Disclosure**. Information disclosure is the unwanted exposure of private data (e.g., a user viewing a table or file the user is not authorized to open, or a user monitoring data passed in plaintext over a network). Some examples of information disclosure vulnerabilities include hidden form fields or comments embedded in Web pages that contain database connection strings and connection details. Any of this information can be very useful to the attacker.
- **Denial of Service**. Denial of Service is the process of making a system or application unavailable. For example, a denial-of-service attack might involve bombarding a server with requests that consume all available system resources or passing the server with malformed input data, which can crash an application process.
- **Elevation of Privilege**. Elevation of privilege occurs when a user with limited privileges assumes the identity of a privileged user to gain privileged access to an application. For example, an attacker with limited privilege might elevate his or her privileges to compromise and take control of a highly privileged and trusted process or account.

MITA will develop a preliminary threat model for each service value chain and make it available to States for adaptation and extension. The Service Threat Modeling Process is adapted from the Microsoft process, with extensions and integration with the service value chain analysis

activities, along with role engineering and multiattribute decision criteria. The key construct is the service diagram that defines the services used and those provided by the systems and people who are involved in an electronic or electronically supported service delivery. Many of the processes include people making decisions and taking manual steps, while others are nearly fully automated except for exception processing. The service delivery defines the business process involved in delivering these services and the composition of these business services into composite services known as *service contexts* can introduce addition threats.

A service context may be for employees performing different roles, or the contexts for the customer, citizen or beneficiary to look up the progress of an authorization or a claim status. It may also be an interface provided to service the needs of a partner agency or to share summary or exception information based on a one-time or ongoing need for notification, such as information required by public health.

The threat modeling process consists of the following steps:

1. Identify assets along a service value chain and define the roles and required privileges of persons involved in delivering that service.
2. Create a Service Architecture Delivery Model for each service channel.
3. Decompose the service application and annotate with S&P integration points.
4. Identify threats (a list of standard threats is provided, but many applications can introduce new threats).
5. Document threats by gathering them into the recommended threat tool.
6. Rate threats by using a risk rating, based on asking the following questions:
   - How bad would the damage be if someone exploited the vulnerability? (Damage Potential)
   - How easily can someone reproduce the attack? (Reproducibility)
   - How easily can someone launch an attack? (Exploitability)
   - Approximately how many users would be affected? (Affected Users)
   - How easily can someone find the vulnerability? (Discoverability)
7. Perform multicriteria countermeasure analysis.
8. Summarize residual threats.

S&P decisions will be made based on threat-driven scenarios and associated impact and value assessments.

## Security and Privacy Model

MITA developed an S&P Goals and Policy Model, shown in **Figure 7-16**, by gathering security goals and policies from various government documents.

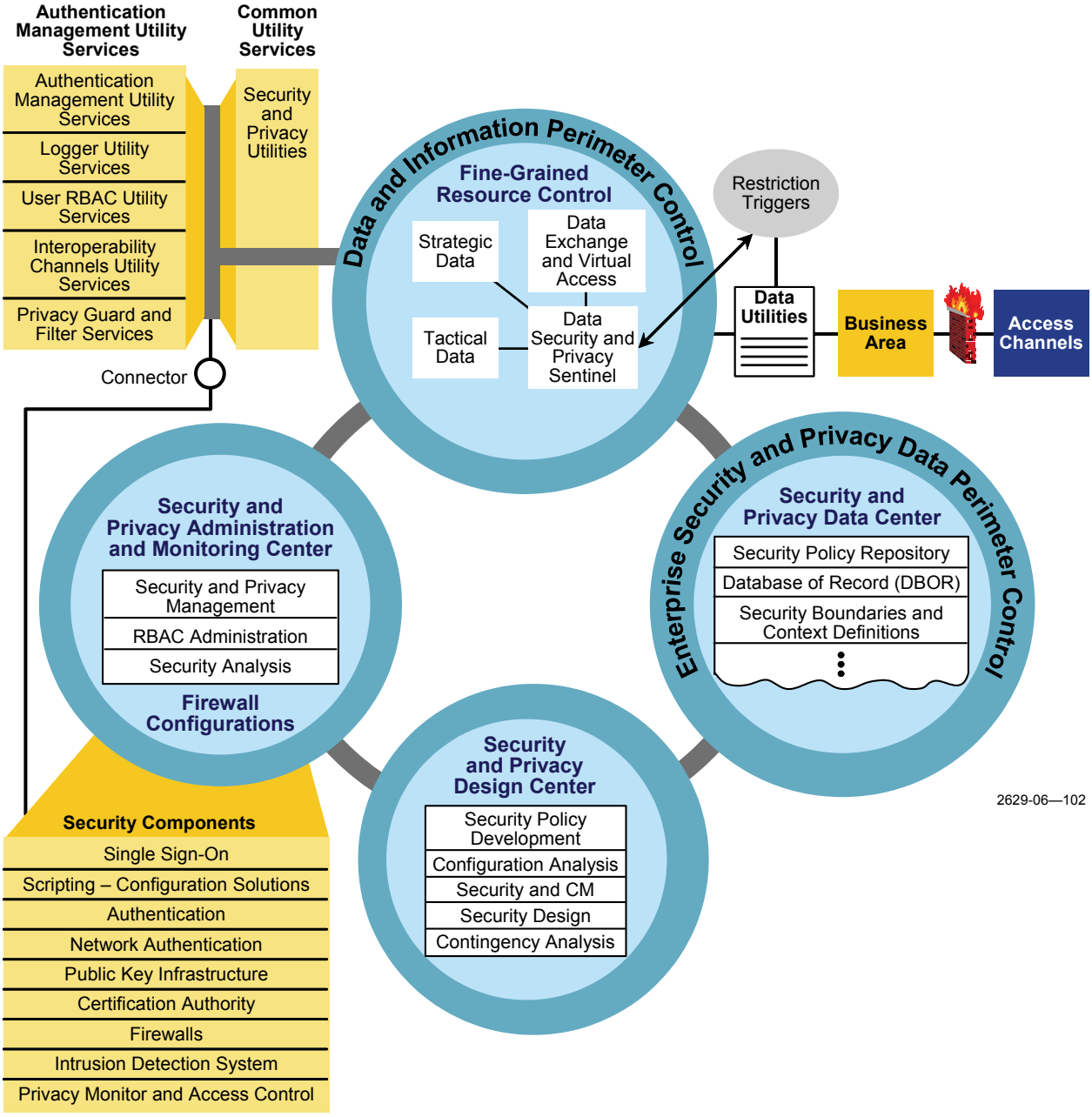



*Figure 7-16. S&P Goals and Policies*

The original purpose of the S&P Model was to define perimeter controls and create security zones around key assets (e.g., the strategic, tactical, and data sharing hubs). Perimeter control capabilities include external firewalls with perimeter controls around critical resources. Strategic, tactical, and data sharing hubs must be protected, as must security components and S&P-related data.

Four separate areas manage S&P capabilities:

- The S&P Design Center specifies S&P elements and policies.
- The S&P Data Center manages data related to roles, responsibilities, and policies.
- The S&P Administration and Monitoring Center is the focal point for operating the protection mechanisms that are in place and responding to threats immediately.
- Fine-Grained Resource Control integrates S&P rules with data to support automated tracking access to individual data.

MITA is packaging security capabilities in the form of COTS components that States can adapt based on their policies and configurations. Those S&P components must be integrated into the business and technical models at the S&P connection points. The security components are defined and linked with S&P utility services that States can integrate with their business area processes and related components.

S&P components will include the following:

- **Single Sign-On.** The ability to sign on to MITA and access the strategic, tactical, and data sharing coordination hub
- **Scripting-Configuration Solutions.** Administrative tools used by authorized State and Federal contractor security administrators
- **Authentication.** The ability to determine the authenticity of a person who seeks access to tactical, strategic, or data sharing hubs (e.g., through Public Key Infrastructure, Certification Authority, or Registration Authority)
- **Network Authentication.** The ability to control interoperability channels and protect the communication for inter-State and national communication
- **Firewalls.** Firewalls that can be dynamically configured
- **Intrusion Detection System.** The ability to detect and flag behaviors that might indicate a security threat or violation
- **Privacy Monitor and Access Control.** The ability to protect private data and log and report any disclosure

MITA will develop S&P utilities that will bridge business areas and S&P components. **Table 7-6** below shows the initial set of S&P utility services and features and the connections to the related components.

### *Table 7-6. Security and Privacy Utility Services, Features, and Connections to Related Components*

| S&P Utility Service | Features | Special Characteristics | Related S&P Component |
|---|---|---|---|
| Authentication Management Utility Services | Passes the business area, user/State identification, and responsible security and development person to the authentication component | Different data types may require different levels of authentication. | Authentication |
| Logger Utility Services | Provides a consistent approach to logging information<br>Provides controls that can increase or decrease logging levels | Logging information will be sent to the S&P data center. | Audit system |
| User RBAC Utility Services | Connects roles to business areas, users who requested services, and context the user works in | Constraints will be defined based on separation of responsibilities (a key area that States must adapt as they add and change people). | S&P Data Center |
| Interoperability Channels Utility Services | Each interoperability channel and access channel will have rights of access defined.<br>These functions will be mapped to the RBAC utilities. | Utilities can detect mismatches of rights; those will be reported.<br>Ability to reconfigure and change the interoperability channel definition files. | Firewalls<br>Intrusion and Detection Center |
| Privacy Guard and Filter Services | Certain data and information will have specific additional privacy and filtering services because of their value. | Attached to subject data areas and selected types of access rights. | Privacy Guard component |

S&P Administrative and Management functions have three components:

- Enterprise S&P Data Center
- Operational monitoring of MITA S&P Administration and Monitoring Center
- The S&P Design Center

These functions were separated out for protection purposes and to provide a "defense in depth" strategy. Separate firewalls would be used for each. The critical resource is the data and the S&P information about the data.

Data and Information Security will use fine-grained security labels with the data hubs and include special resource access triggers that will be integrated with utility services.

## Concerns and Challenges

### Cross-Agency Concerns

The cross-organization nature of the data and services shared among the Medicaid and other medical communities raises several critical issues that MITA is addressing with specific "best-for-now" approaches that will appear in modules and are subject to change. The MITA team will present these issues to the Architecture Review Board regularly and discuss any residual threats. Some issues may cause inefficiencies and create undesirable labor-intensive activities.

- Policy alignment
- Federated identity management along the channels
- Exception management and control
- Policy and metadata-driven S&P (common metadata elements for S&P)
- Management and control aspects
  - Flood of logons have occurred
  - Message traffic not deliverable
  - New vulnerability detected
- Adaptability and flexibility — change scenarios
  - Change to roles and responsibilities
  - New service added
  - New data container authorized to be shared
- Security standards framework
  - Policy Layer: WS-Policy, WS-Trust, WS-Privacy, Security Assertion Markup Language (SAML), Enterprise Privacy Authorization Language (EPAL)
  - Federation Layer: WS-SecureConversation, WS-Federation, WS-Authorization, XML Key Management (XKMS)
  - Mechanism: Extensible Access Control Markup Language (XACML), XML-Encryption, XML-Digital Signatures, Extensible rights Markup Language (XrML)

### Challenges

S&P must be integrated throughout the architecture. S&P experts must understand and support the mission and business goals of MITA.

Some of the key challenges include:

- **Inconsistent or nonexisting guidance.** NIST guidance is not consistent with e-government transformation needs.

- **Complexity.** S&P technology is complex and multilayered and must be integrated from the beginning.
- **Threats.** New threats must be addressed immediately and yet accommodate new and changing technologies (such as WS), while promoting security infrastructure reuse.
- **Enterprise Security Perspective.** Migration from a system perspective to an enterprise perspective must include modifying the "virtual enterprise" business model to blur boundaries so that "outsiders" become "insiders."

## Enterprise Security and Privacy Data

Security components and managing S&P components are data-drive critical processes. Data must be defined, mapped to other subject data models, and protected. Enterprise S&P data are shown in **Figure 7-17**, and the data elements are defined below.

The Database of Record Meta Recovery Index addresses recovery of tactical and strategic data in cases of security violations. The Index will include elements such as security log files within the S&P utilities and the following:

- An S&P policy repository that will define the agreed-on S&P policies, using an English language agreement and declarative S&P policy languages (e.g., SAML and OPAL).
- Definitions for S&P boundaries or zones, including any DMZ or firewall areas that have been established.
- Security configuration repository elements, including security components that will map security patterns to vend products and security capabilities offered and those MITA uses.
- An application asset repository that will include an S&P template assessment to identify risks for each business area and portion of a business area. The repository will initially be in the form of a template, and diagrammatic models will be added later.
- A threat repository that will capture threats that the architecture addresses and other threats that should be considered.
- A vulnerability repository that will include computer vulnerability evaluation forms classified on the basis of security standards and mapped to the MITA business and technical models.
- S&P patterns and icons that MITA will define using a common pattern template. This portion will be open to all.
- Summary S&P notification and guidance, which will be open to all and based on an ongoing communication effort. S&P must be part of the MITA culture and process. One of the announcements will be a roles-and-responsibilities notification, including to specialists on certain security components (e.g., firewalls, intrusion detections, and directories).

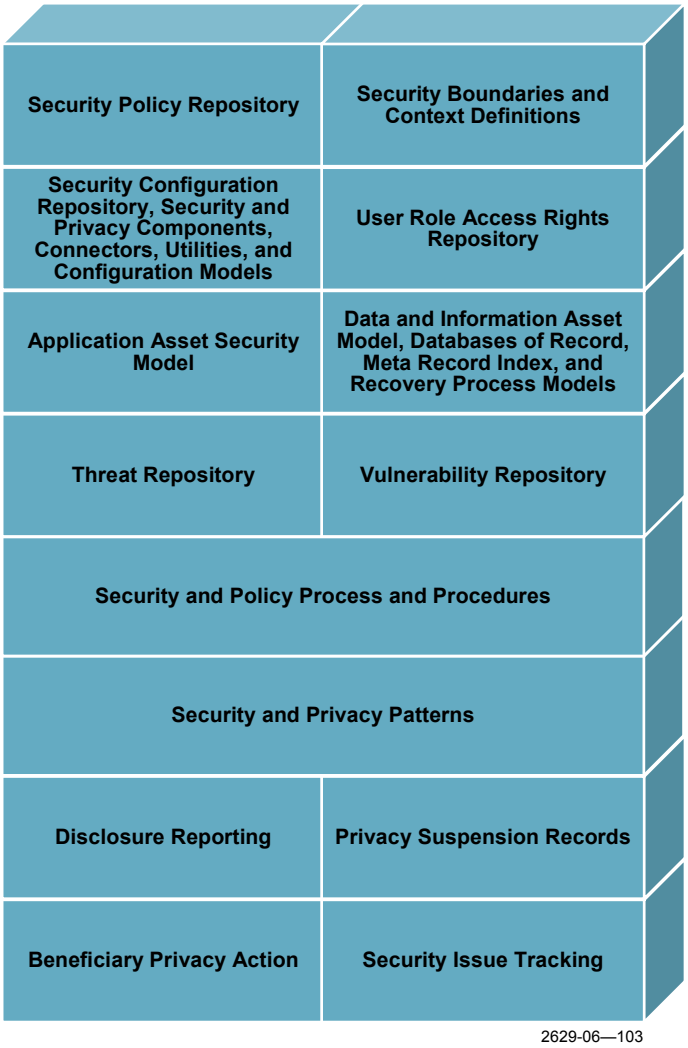



*Figure 7-17. Security and Privacy Data and Information Subject Area Model*

## Security Levels

For each major element of security, three levels of S&P have been defined initially:

- Level 1 — basic level
- Level 2 — mid level
- Level 3 — advanced level

The levels include the following:

- Application Security Levels
- Data and Information-Supported Security Levels

### Interoperability Channel Levels

The S&P Portfolio will coordinate the refinement of these models and the establishment of the capabilities needed for each level, as discussed in **Table 7-7**.

*Table 7-7. Security and Privacy Questions and Answers*

| Question | Answer |
|---|---|
| Why is the S&P model important to MITA? | The S&P model shows a consistent way of implementing security across the network. Key concepts are single sign-on/log-in, use of standards, and a wide range of security components. |
| Who should understand the S&P model? | Designers and implementers of systems and networks should review the model to ensure that it has addressed all appropriate levels of security. |
| How will the S&P model be used? | The S&P model offers many implementation options. System designers and implementers should review it and select components appropriate for data sharing and for access needed to meet business needs. |
| How will the S&P model be refined and updated? | The S&P Portfolio team will update the S&P model. Further details, including detailed specifications and minimum-security requirements, will be provided in coming years. |
| How will the S&P model support ongoing business decision making? | New IT procurements should specify the appropriate security components to support data sharing. |

## How Do MITA Services Interact with the MITA Infrastructure?

This section provides two examples of MITA services and the MITA infrastructure — specifically, adding a MITA service to the enterprise and invoking a MITA service.

### Addition of a MITA Service

A State must perform the following steps to add a new MITA service to its infrastructure, as shown in **Figure 7-18**:

- **Step 1.** Establish a Business Service Connection by defining service endpoints (i.e., providers and consumers) and entering into a Business Interoperability Agreement. A Business Interoperability Agreement is a contract between two or more agencies in a State or between a State agency and another organization that involves a business area (e.g., a State agreement with CMS on Medicaid, with the Centers for Disease Control and Prevention [CDC] on vaccines, or with the Food and Drug Administration [FDA] on adverse drug event reporting). MITA will provide States with a Business Interoperability Agreement Template that relates a business process to a "partner link," as defined in BPEL, and to another business area or collection of services. The purpose of a Business Service Connection is to encourage *intra*organizational and *inter*organizational interoperability.

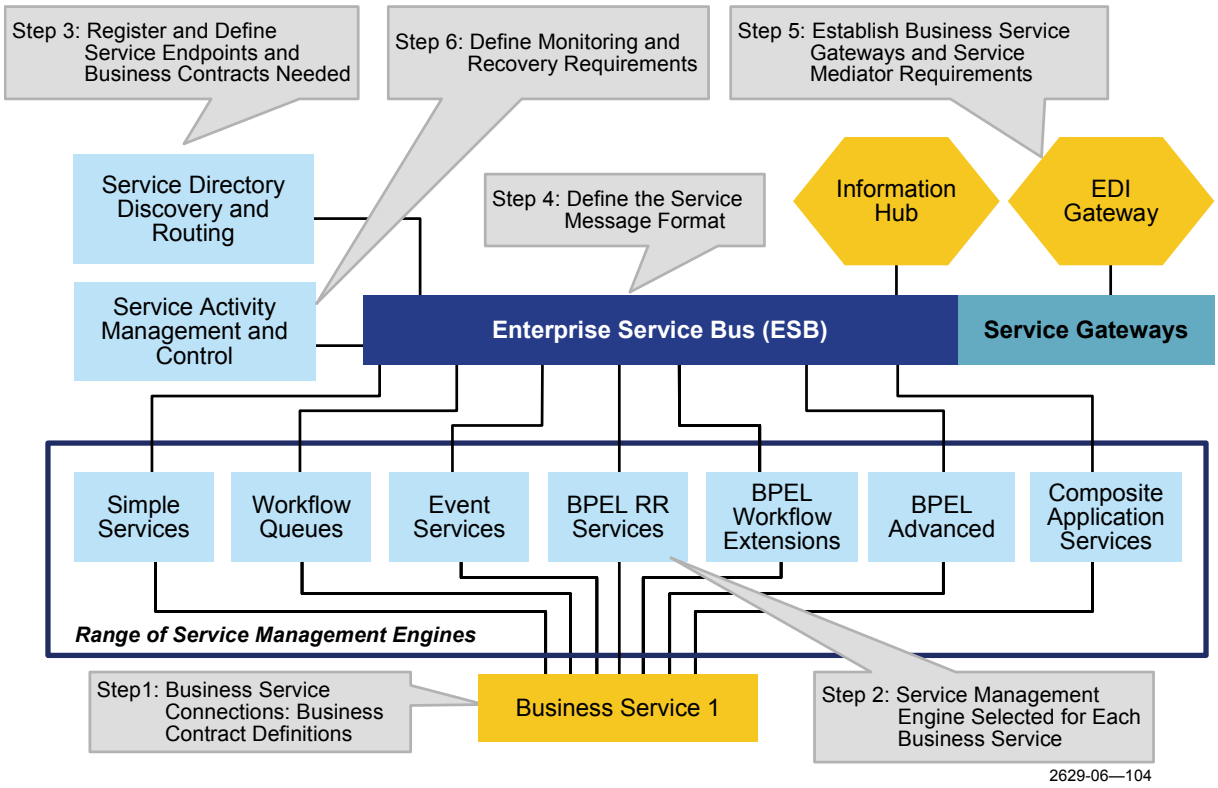



*Figure 7-18. Service Infrastructure — Adding a Business Service*

- **Step 2.** Select the kind of SME that meets the service patterns and the behaviors of the State.
- **Step 3.** Define and register the service with a Universal Description, Discovery, and Integration Version 3 (UDDI 3)-compliant registry that other community registries can link to. Such a registry will allow the semiautomated discovery and binding of service requests to specific service endpoints and provide information needed to route the service message format to the business and technical service endpoints. The metadata will include a definition of channels, links between business process models (in BPEL) and the messages exchanged, service endpoints, and service contracts as defined in WSDL. (See the Data Management and Access Service sections for Interoperability Data Element Definitions that are related to each of the WS Standards elements.)
- **Step 4.** Define the Service Message Format. The ESB will use a generic data format and specific content formats MITA will define and capture in a semiformal template (the Data Exchange and Sharing Interchange Template) and in a more formal self-describing XML-based Information Exchange Package. The Package will include both WSDL and XML Schema (although the implementation might not send in the XML format but rather in the more compact binary format). These documents and their generated formats will allow for easy adaptation and semiautomated testing. Tests will

come from service or business contracts and are extended, with additional tests developed by testers. Test tools for end-to-end services are critical aspects of service testing and incremental release of services.

- **Step 5.** The Service Gateway will use the metadata from Step 2 to establish the bindings and define the needs for service mediation between outside interfaces, such as the EDI Gateway, or as a link between other ESBs.
- **Step 6.** Monitor cross-services and executive recovery. MITA will monitor the performance of service capabilities as it adds them and will support their recovery. Exception reporting, performance measurement, and recovery are built into individual service-enabled products. These features are desirable at Level 3. End-to-end activity, management, and recovery capability will be expected at Level 4. The script that defines the automated and manual steps to recover from failures is a key element of a complete service solution.

## MITA Service Invocation and Execution

After MITA has added a service to the MITA infrastructure, States must perform several steps to activate the service. These steps are set forth below and shown in **Figure 7-19**.

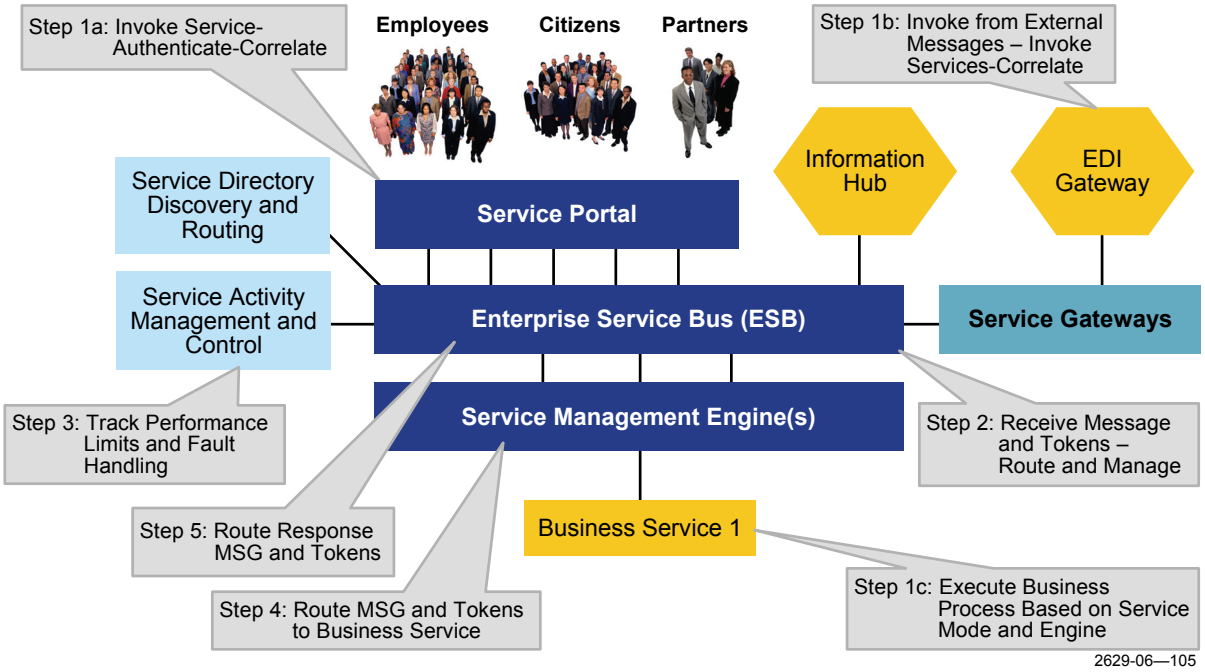



*Figure 7-19. Service Infrastructure — Service Invocation and Execution*

- **Step 1. Service Invocation**

  States can invoke MITA services in three ways:

  (a) *Invoke Service, Authenticate, and Correlate.* This refers to a user at the portal invoking or reinvoking a service that the person had been using, including providing enough information to correlate the service to common activities and start up where the user left off. The user must sign on and be authenticated before starting up the service, at which time the eAuthentication service will establish a token that will note the user's roles and authorizations. The service will then establish another token for the types of services the user will be working on by pointing to the work or processes and activities that ended at the last session.

  (b) *Invoke from External Messages, Invoke Services, and Correlate.* This initiates a set of services, such as sending in batch messages for all transactions for the day. Batches of service requests will be managed by the series of threads that will result in a stream of interactions. The ESB and the service portal can handle multiple threads of interaction and can be configured based on performance needs. External messages will come through this path individually or collectively from a partner organization or another agency.

  (c) *Execute Business Process Based on Service Mode and Engine.* These are the business services themselves, which can interface with one or more of the service engines and range from simple to complex and composite applications. This is a message that comes from a business service to another business service.

- **Step 2. Receive Message and Tokens, Route, and Manage.** The ESB is a key linchpin between the different forms of services from the three major sources in Step 1. The message is received, a token is related to the service type (correlation set), and an S&P token is attached to the message. It is used for routing and managing the service flow. Some services are more important and other message flow capabilities (e.g., prioritization and alternative path routing depending on performance limits).
- **Step 3. Track Performance Limits and Fault Handling.** This is to ensure that performance policies and agreements are followed and to address fault handling related to end-to-end recovery and the measures needed to maintain the quality of service levels.
- **Step 4. Route Message and Tokens to Business Service.** The SME routes the message and tokens to the appropriate business service.
- **Step 5. Route Response Message and Token (Optional).** If a response is generated by the business services, it is routed to the appropriate service based on predefined orchestration.

## How Do States Use the MITA Application Architecture?

The MITA AA should be used as a reference document that identifies the components needed for the infrastructure of the Medicaid enterprise and as a requirements document that provides details for a State's Medicaid enterprise infrastructure. States can use the document in this capacity as a source for their Advance Planning Documents (APDs) and RFPs.

## How Do States Participate in Developing the MITA Application Architecture?

States participate in developing the MITA infrastructure by taking the following actions:

- Participating in working groups to define common application architecture requirements (e.g., audit, logging, and performance management)
- Providing State Medicaid lessons learned from State enterprise architectures related to the MITA AA
- Providing potential personalization points for the MITA AA
- Providing candidate issues and concerns related to the MITA AA
- Submitting proven solutions as candidates for MITA standards
- Helping to define standards for the MITA infrastructure
- Submitting details into a repository as a MITA solution set

## Conclusion

The MITA AA guides States in assembling their Medicaid enterprises to ensure that they are interoperable and plug-and-play capable. The current version of the MITA Framework defines an initial AA. Future versions will be more specific as to AA component requirements, such as SMEs, ESB, and hubs. State Medicaid enterprises will evolve to optimize MITA's adaptability, flexibility, interoperability, and data sharing — an evolution that will promote major improvements in policy, decision making, and day-to-day operations.