Part III – TECHNICAL ARCHITECTURE

Chapter 5 – APPLICATION ARCHITECTURE

Table of Contents

List of Figures

List of Tables

Introduction

Previous chapters discussed Medicaid IT Architecture (MITA) business services and technical services. These services are central to the MITA Framework; however they are not an integrated solution by themselves. Integrated solutions include middleware, traditional technologies, or provide a mechanism for application integration and reusable components. This section discusses the MITA Framework Application Architecture (AA) a component of the MITA Technical Architecture (TA). The MITA TA approaches application integration using a Service-Oriented Architecture (SOA). The MITA Framework integrates its business services with its technical services through service elements that the State Medicaid Agency (SMA) configures as a service layer. Using SOA as an integrating framework allows services to remain both platform and technology independent and yet remain interoperable.

MITA provides platform- and technology-independent services by specifying their message structure, the business logic of the service, and the abstract portion of the service's interface. The SMA is responsible for defining the concrete portion of the service's interface based on their specific environment.

The topics covered in this chapter include:

- Application Design Principles and Patterns
- Application Architecture
- Application Architecture Key Components
- Security and Privacy
- Services and Infrastructure Interaction

Purpose

The MITA Framework AA defines the relationship between end users, services, and infrastructure. It also provides guidance to the SMA on how to connect services and infrastructures to improve services for end users.

Scope

MITA provides a framework for the AA that guides the SMA through the System Development Life Cycle (SDLC) and advancement of Information Technology (IT) capabilities to higher maturity levels.

The MITA AA goals include:

- Creating an infrastructure for effectively developing and using a service-driven architecture to use services effectively.
- Mapping technology standards to components.

- Defining patterns for components States use as templates for design and development. The AA does not address deployment specifics, such as Commercial Off-the-Shelf (COTS) products, specific performance standards (e.g., bandwidth or million instructions per second [MIPS]), software components, or object classes.
- Extending services to include compatibility with Health Information Exchanges (HIE) and Health Insurance Exchanges (HIX).
- Guiding States through the process of identifying and developing the physical networks and hardware based on their specific environment.

Application Design Principles and Patterns

The State Medicaid Enterprise is a very large and typically tailor-made conglomerate of software built from diverse components. States serve large transactional workloads and scale along with the enterprise they support, readily adapting to changing business realities. Scalability, correctness, stability, and extensibility are the most important concerns when architecting such systems.

There are many challenges in creating software systems that can meet the demands of the typical State Medicaid Enterprise that require advanced degrees of quality, reliability, and functionality while performing at acceptable levels. The complexity of these systems are increasing at an alarming rate and is now requiring a Medicaid AA that follows sound development principles and design patterns.

Application Architecture Design Principles

Abiding by a set of well-defined application development design principles is a sign of a comprehensive application environment. While there are general programming best practices like programming to an interface to decouple dependencies within an implementation, the modern-day Medicaid Enterprise requires the SMA to use the AA design principles as driving concepts for building a sophisticated system for future expansion.

Four (4) well-known example application design principles at an enterprise level include:

- **Data Normalization/Factoring** – Since duplication leads to errors, there is a strong push to establish Single Source of Truth (SSOT) entities to achieve the goal that each fact be a single non-decomposable unit where these facts are independent of all other facts. The expectation is when a data change occurs, only one data location needs modification. This principle is well known to database designers, but also applies less formally to an application, under the name factoring. Well planned architectures determine and execute on localizing information and behaviors. At runtime, this manifests as layering, the notion that a system may factor into layers, each representing a layer of abstraction or domain.
- **Automatic Propagation** – Consists of the need to maintain consistency and correctness by propagating changes in data or code across a modular environment. In other words, when it is necessary for performance sake to duplicate data or application code to maintain consistency and correctness, propagation of these facts is automatic at the time of construction.

- **Minimize Functionality** – If an application component exists that meets requirements, it is a best practice to reuse wherever possible. This practice provides the benefits of less code to write, verify, and maintain, and it ensures that the code will occupy less memory at runtime.
- **Construct Layers** – In order to construct an extensible system, the construction process involves the use of intermediate layers capable of acting on the data received from higher layers of the AA. These intermediate layers act like virtual machine engines that handle the processing of a specific function in a separate session. This permits data to define the specific functionality, allowing the layered components to be highly reusable.

Some principles highly interrelate. For instance, data normalization works only if there is automatic propagation, which in turn, is effective when the architecture takes construction into account. Moreover, combining minimal mechanisms with the notion of constructing a layered environment means that the AA usually features a limited set of patterns that enable construction of arbitrary system extensions (expansion by pattern).

Application Architecture Design Patterns

Patterns are repeatable configurations of elements. In an enterprise-sized application system, patterns are complex combinations of architecture elements that provide a repeatable design. Enterprises leverage patterns for expanding their operations in a reliable and repeatable manner. At the same time, they exploit location differences to customize patterns for better fit in areas where such diversity is important. For example, developing an Enterprise Architecture (EA) enables an enterprise to identify and use patterns in supporting standardization efforts, improving business processes, or scaling operations.

There are established application design patterns and commonly used development languages for SOA. There are design patterns for practically every aspect of computing (i.e., Oracle Java, Microsoft.NET, data model transformation, etc.). Developers may use coding conventions and notations to document pattern content for consistency purposes. Where possible, the MITA team recommends having all development staff, groups, and external vendors using the same design patterns to establish continuity of components. This is common practice since there are benefits of time savings and reduction of risk associated with effective pattern usage.

Application Architecture

The MITA AA connects MITA business services with technical services, as shown in **Figure 5-1**. The SMA will tailor MITA business services to environmental needs. Business services have a common core for all MITA processes that adapts and extends to meet States' special policies, rules, and deployment requirements. The MITA Framework defines its services from the abstract level to the design level of the SDLC. This allows the SMA to build service interfaces as standard interfaces without dialects caused by interpretations.

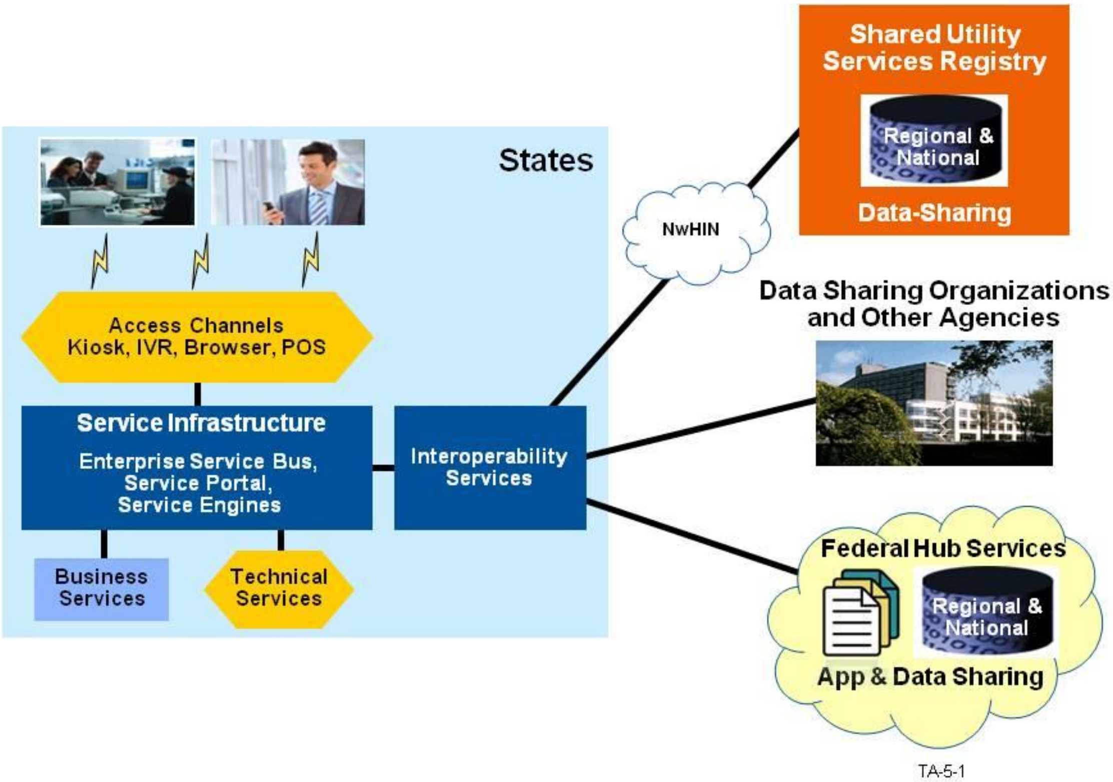

Figure 5-1. Conceptual Technical Architecture Diagram

The service infrastructure uses standards-based elements that allow intrastate service process integration and data sharing with other organizations and agencies. The MITA Framework is compatible with the Federal Health Architecture (FHA), the Nationwide Health Information Network (NwHIN), regional and national shared data sources, and the network on Regional Health Information Organizations (RHIOs). The MITA Framework defines a series of interoperability services based on Web Services (WS) and Extensible Markup Language (XML) message formats and protocols. The tools the SMA needs to establish interoperability, data capabilities, and other support requirements are available individually to the SMA in groups using common facilities.

The following sections provide a description of the top-level MITA SOA. They describe fundamental infrastructure components, such as the Enterprise Service Bus (ESB), the Service Management Engine, infrastructure services (e.g., external data-sharing and hubs), and provide references to industry standards.

Components of Application Architecture

A multilayer AA model represents a combination of MITA applications and connections to deliver services to stakeholders, as shown in **Figure 5-2.** The four (4) levels are the Access Layer, Service Management Layer, Service Application Layer, and Platform Layer.

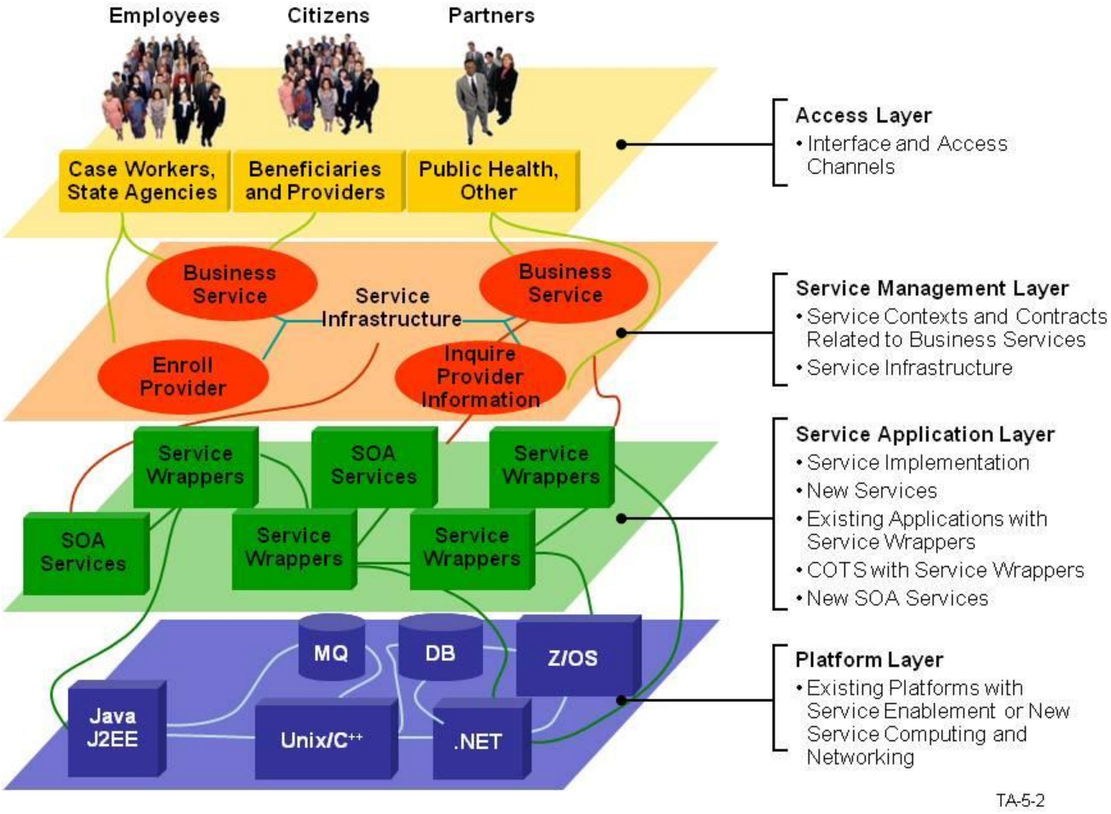

Figure 5-2. Multilayer Application Architecture Model

- **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. Employee interfaces have more capabilities with services that are specific to one or more assigned employee roles. Nonemployees 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. The Access Layer also restricts business partners’ interfaces to agreed-upon business service contracts for information exchanges, sharing, and specific services.
- **Service Management Layer** – Consists of the service infrastructure, service contexts, and service contracts for each business service (e.g., Determine Provider Eligibility and Enroll Provider) and provides a view into business services as they relate to roles and task assignments. The Service Management Layer links to the application layers, either directly or through service wrappers.

- **Service Application Layer –** Consists of services a Medicaid Enterprise uses. Although the MITA Service Application Layer consists of services, those services might be new services, wrapped legacy applications, or wrapped COTS products. Business services and technical services integrate with newly defined services. The Service Application Layer evolves incrementally. Applications run on the same platforms, with new features that permit service enabling while providing some new service computing and service networking capabilities.
- **Platform Layer –** Existing services, new service-computing capabilities, and new service-oriented networks evolve, depending on the performance and reliability needs of each state. The MITA AA standardizes the Access Layer, the Service Management Layer, and the service wrapper definitions of the Service Application Layer. The SMA is responsible for the Platform Layer and the implementation within a service wrapper in the Service Application Layer.

Building Services

To illustrate how stakeholders build service application services, **Figure 5-3** depicts some of the fundamental pieces of a SOA-based business service. Each service has Interface Components that include security attributes that inspect incoming messages to verify the message originator has authorization to invoke the service (e.g., only designated Medicaid staff members have authorization to approve claims.)

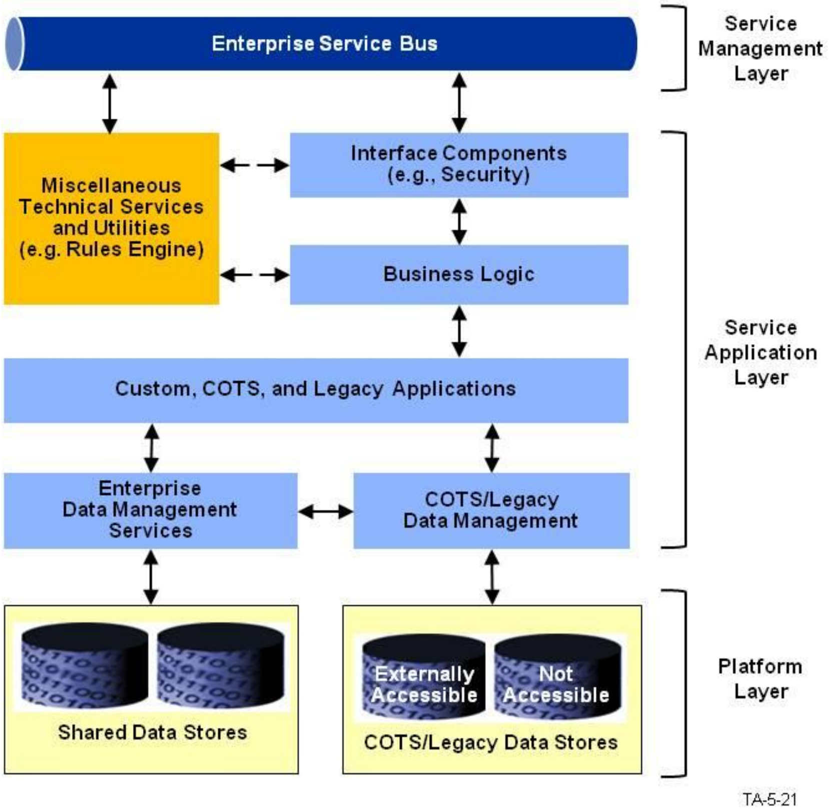
Enterprise Service Bus
Service Management Layer
Miscellaneous Technical Services and Utilities (e.g. Rules Engine)
Interface Components (e.g., Security)
Business Logic
Custom, COTS, and Legacy Applications
Service Application Layer
Enterprise Data Management Services
COTS/Legacy Data Management
Shared Data Stores
Externally Accessible
Not Accessible
COTS/Legacy Data Stores
Platform Layer
TA-5-21

Figure 5-3. The General Structure of Business Services

The Business Logic portion of the business services examines the received message and coordinates the execution of underlying custom, COTS, or legacy applications to provide the necessary business results for the received message. The business logic process accesses miscellaneous enabling technical services to perform its processing responsibilities.

The applications portion of the business services accesses and uses a set of enterprise data management services to provide uniform access to data by using standard definitions for all shared and externally accessible data in the State Medicaid Enterprise. Data contained in COTS and legacy systems requires special handling. In the case of legacy data stores, data access routines tend to be specific to the underlying technology. Data stores used by COTS packages often have proprietary data structures; data access routines and only vendor-approved Application Programming Interfaces (API) access them. In addition, not all COTS data stores are externally accessible, not even via API. The enterprise data management services provide transparent data management services to all accessible data stores in the State Medicaid Enterprise. The data access services are platform independent, so that, as legacy systems phase out, or technical staff restructures databases, no changes to the enterprise data management services are visible to the consumer.

Using SOA standard application methods, systems invoke services at different architecture layers. To maximize reuse across the State Medicaid Enterprise, the SMA standardizes the service descriptions, invoking messages for all of the services connected to the ESB, and as many of the lower level technical services as possible.

Application Architecture Key Components

Figure 5-4 depicts the relationship between the MITA infrastructure and services. Business and technical services link by service infrastructure elements using the important 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."

There is currently no universal agreement within the industry regarding the components and functionality of an ESB. The MITA Framework concept of an ESB follows Chappell's definition and includes common elements and those critical to linking business services and technical services.

The service integration and interoperability methods provide loose connectivity and are essential enablers of flexibility. The consistent use of this service approach is an important element to designing the SOA. The significant components of the MITA AA are:

- ESB and Access Channels
- Service Management Engine

- Service Gateways and Mediators
- Distributed Computing and Data Access
- MITA Framework Documents
- Interoperable Services
- Security and Privacy (S&P)

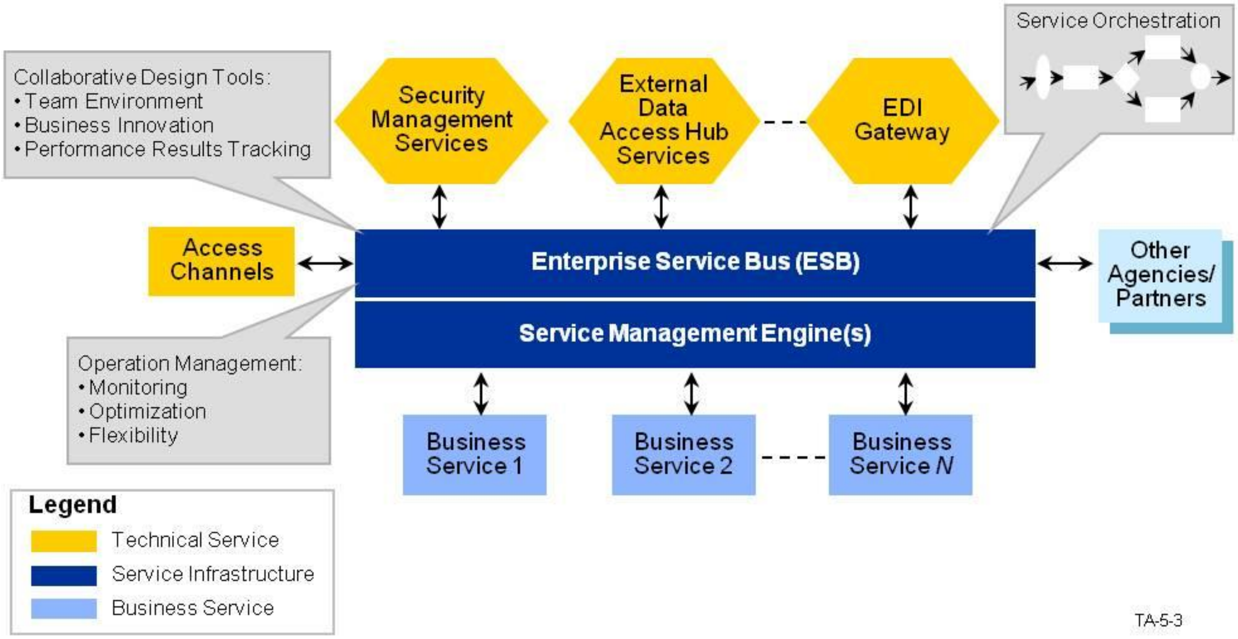

Figure 5-4. Service Infrastructure

Enterprise Service Bus and Access Channels

An ESB is an infrastructure component that supports the Modularity Standard. This standard addresses the:

- Use of SDLC methodology.
- Identification, description, and use of adaptable and open interfaces.
- Use of business rules engines for rapid response to program changes.
- Submission of those standardized business rules definitions to future design repositories to support collaboration.

Traditionally, users accessed or linked to systems using proprietary formats of individual vendors, developers, or integrators, thus making systems more complex and hindering interoperability and integration. The MITA AA addresses this issue through Access Channel Services, shown in **Figure 5-5.**

Access Channel Services provide the specific device-handling types. Each Access Channel Service handles unique features of each device.

The access channel routing and management capability ties into the security boundary protection services, accesses other S&P services that support single sign-on needs, authenticates users, sets up the Role-Based Access Control (RBAC) permission, and passes a token (or link) to the ESB. The access channel uses a token with the ESB and passes it 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). The access channel carries correlation sets along entirely, but more often it provides a small token to the correlation set information. The ESB or a technical service has the capability of logging and gathering levels of tracking information for exception handling, recovery, and S&P auditing.

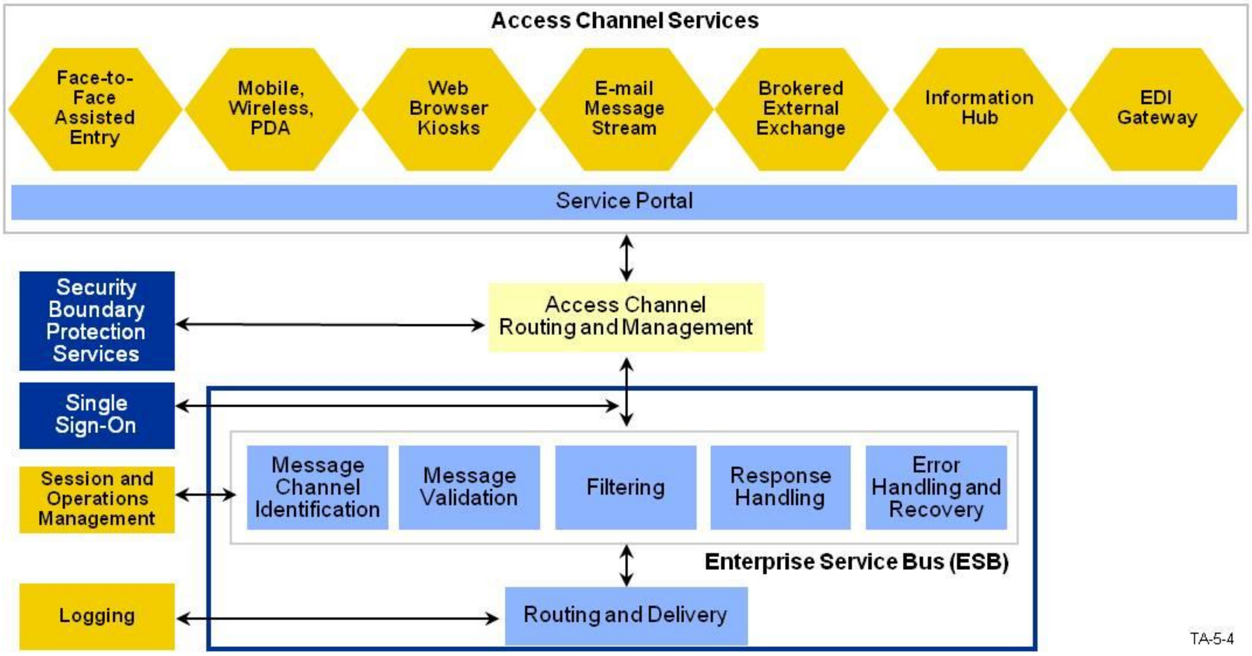
Access Channel Services
Face-to-Face Assisted Entry
Mobile, Wireless, PDA
Web Browser Kiosks
E-mail Message Stream
Brokered External Exchange
Information Hub
EDI Gateway
Service Portal
Security Boundary Protection Services
Access Channel Routing and Management
Single Sign-On
Session and Operations Management
Message Channel Identification
Message Validation
Filtering
Response Handling
Error Handling and Recovery
Enterprise Service Bus (ESB)
Logging
Routing and Delivery
TA-5-4

Figure 5-5. Enterprise Service Bus and Access Channel Services

Access Channel Services and the ESB fit a range of interoperability issues across business areas to provide cross-organization interoperability services. 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 ties 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 a 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 the service verifies the RBAC permission. 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 allows the user to start where he or she left off.

Many organizations have web portals to facilitate access to their systems. These service portals require an integration manager to handle the human side of the workflow. Automated work queues manage user access through an assigned role. Users may have multiple roles that may require additional queues.

Service portals follow WS standards, such as WS-Remote Portlet standards. Service users 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 endpoint and the business services representing the other end. The service endpoints that are a Uniform Resource Identifier (URI) for service users and service providers, provide the ability to connect in a standardized way as one of the main uses of the service portal. The MITA AA uses WS-Addressing standards for the service endpoints. The service portal represents a natural evolution of the web portal technology. It has capabilities that allow it to interface with the other service infrastructure components. Some of the major capabilities of a web portal are support of web browsers that understand Web Service Definition Language (WSDL) and output to other service elements with service-formatted messages. The portal and portions of the portal are service endpoints.

Figure 5-6 depicts how security tokens integrate into the infrastructure. The user signs on and invokes an authentication and authorization process, consisting 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, then it creates an RBAC.
2. The token tells the ESB the message can transmit and make the connection 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.

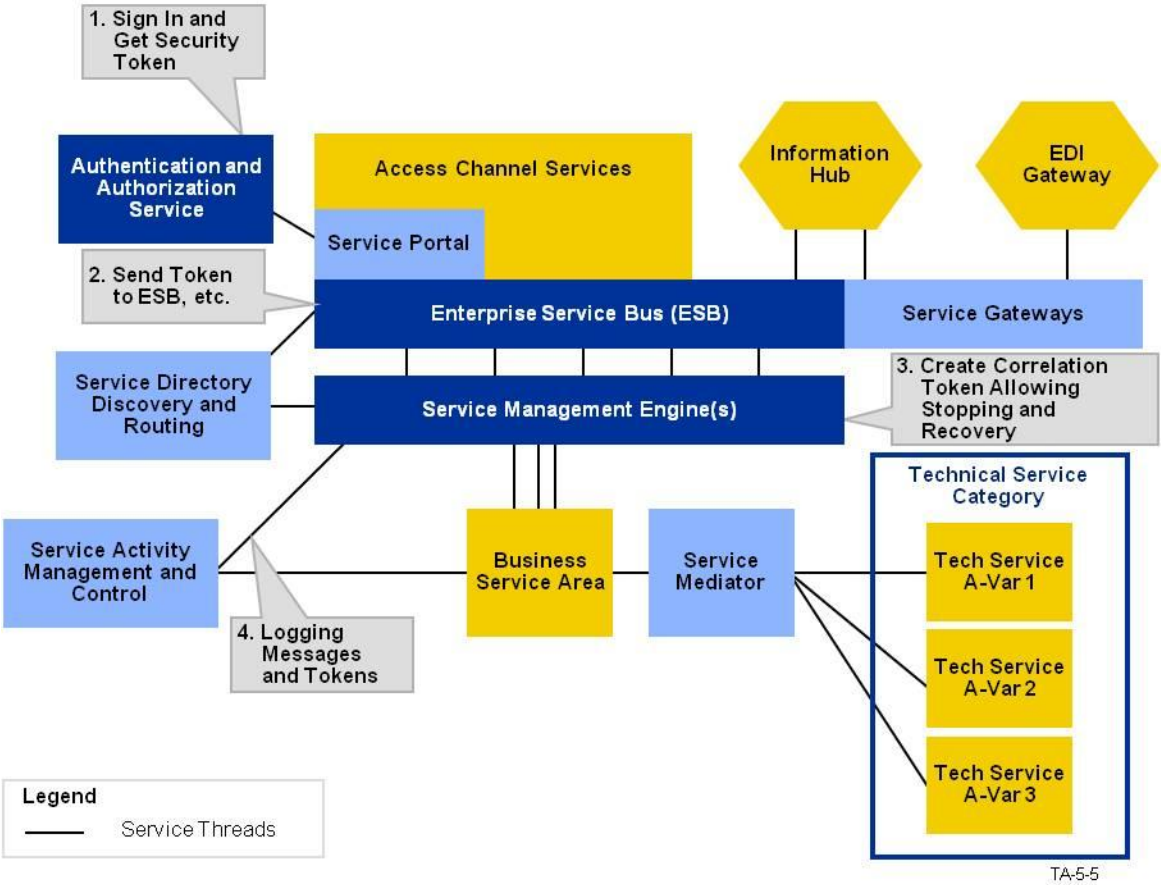
1. Sign In and Get Security Token
Authentication and Authorization Service
Access Channel Services
Information Hub
EDI Gateway
Service Portal
2. Send Token to ESB, etc.
Enterprise Service Bus (ESB)
Service Gateways
Service Directory Discovery and Routing
Service Management Engine(s)
3. Create Correlation Token Allowing Stopping and Recovery
Technical Service Category
Service Activity Management and Control
Business Service Area
Service Mediator
Tech Service A-Var 1
Tech Service A-Var 2
Tech Service A-Var 3
4. Logging Messages and Tokens
Legend
Service Threads
TA-5-5

Figure 5-6. Service Infrastructure's Operation Concept of Security

Service Management Engine

A second fundamental part of the MITA AA infrastructure is the Service Management Engine, shown in **Figure 5-7.** Service management engines are mini-operating systems for a service that manages the execution of the business and technical services. The Organization for the Advancement of Structured Information Standards (OASIS) publishes SOA standards including ESB and service management engines.

The AA Service Management Engine component relates to the business results condition that supports the accurate and timely processing of eligibility and claims adjudication with a high degree of automation; it also supports effective communications among Communities of Interest (COI). States will identify performance standards and evaluation plans to interact with COI for feedback of accessibility, ease of use, and appropriateness of decisions.

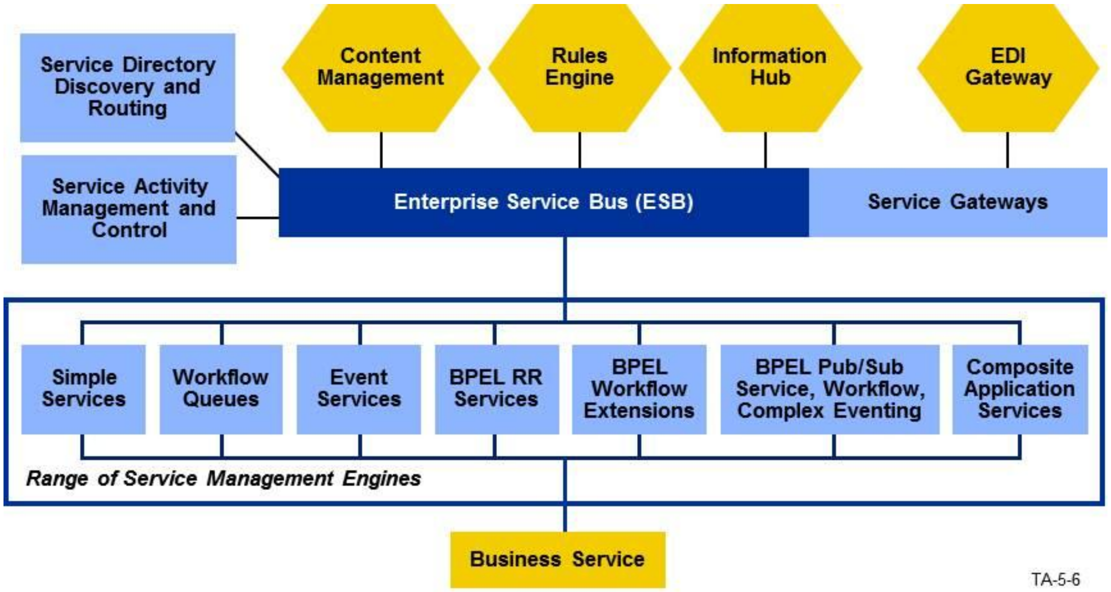
Service Directory Discovery and Routing
Service Activity Management and Control
Content Management
Rules Engine
Information Hub
EDI Gateway
Enterprise Service Bus (ESB)
Service Gateways
Simple Services
Workflow Queues
Event Services
BPEL RR Services
BPEL Workflow Extensions
BPEL Pub/Sub Service, Workflow, Complex Eventing
Composite Application Services
Range of Service Management Engines
Business Service
TA-5-6

Figure 5-7. Service Infrastructure – Service Management Engine

Service Management Engines execute the service contracts defined in WSDL or the more advanced service composition and business process management languages. These engines are diverse and support a range of capabilities. Different services have different service behavior needs from very simple services to complex and composite services. Depending on the SMA need, the business service uses different orchestrations and management of services. Seven (7) types of service engines 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, messages, or cases route 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 has 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 (BPEL) 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 executes and the locations identified in the Business Process Model receive the results.
- **BPEL with Workflow Extensions** – A service that combines BPEL with the ability to integrate the workflow queuing and high levels of workflow management. The Workflow

Management Coalition (WFMC) standards group (Level 4) is defining a common bridge between BPEL and workflow tools.

- **BPEL Advanced** – A service (currently proposed) that includes more advanced BPEL features (Pub-Sub, Service Plus, Workflow, and Complex Eventing).
- **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.

Service Management Engines will incorporate other technical services within the orchestration and workflow processes. Rules Engines and Enterprise Content Management (ECM) are favorable services, as depicted in **Figure 5-7** for usage within the MITA Enterprise. Rules Engines allow for entry of easily configured business logic into the stream of events while ECM services allow entry of different forms of information content in a variety of ways. For instance, the decision management methods included by rules engines provide logic involving the retrieval and manipulation of a database, so database integration through the Service Management Engines becomes critical. Workflow combined with an enterprise content manager will enhance record control to help comply with government regulations such as the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley, PCI DSS, and the Federal Rules of Civil Procedure. Along with publishing SOA standards, OASIS has established Content Management Interoperability Standards (CMIS) to provide uniformity among ECM offerings. These technical services are becoming mission critical components of the Medicaid Enterprise as the computing environment and end-user expectations and needs expand at an alarming rate.

Marketed products exist in each of the categories above. Over the next few years, Service Management Engines are a significant aspect of designing and managing for change, an important aspect of the MITA goal of flexibility.

The MITA team anticipates stakeholders will define more capabilities and new patterns of business processes and workflow.

Service Gateways and Mediators

To deliver services end-to-end, the MITA AA needs a common set of service elements that agrees with set standards, and bridges technologies that address changes and innovation. Those bridging technologies are semi-automatic and sufficiently intelligent to handle many of the common interoperability elements, as shown in **Figure 5-8**. The Service Gateway and Service Mediators are two service elements that currently accommodate this need. The MITA AA uses bridging services to mediate differences because absolute compliance with standards is not realistic.

The 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 HIPAA translators.

The Service Mediators provide a common service contract and service message interface that translates specific vendor offerings. Although three (3) different products may have similar capabilities and a service interface, they may differ slightly. Service Mediators handle those differences.

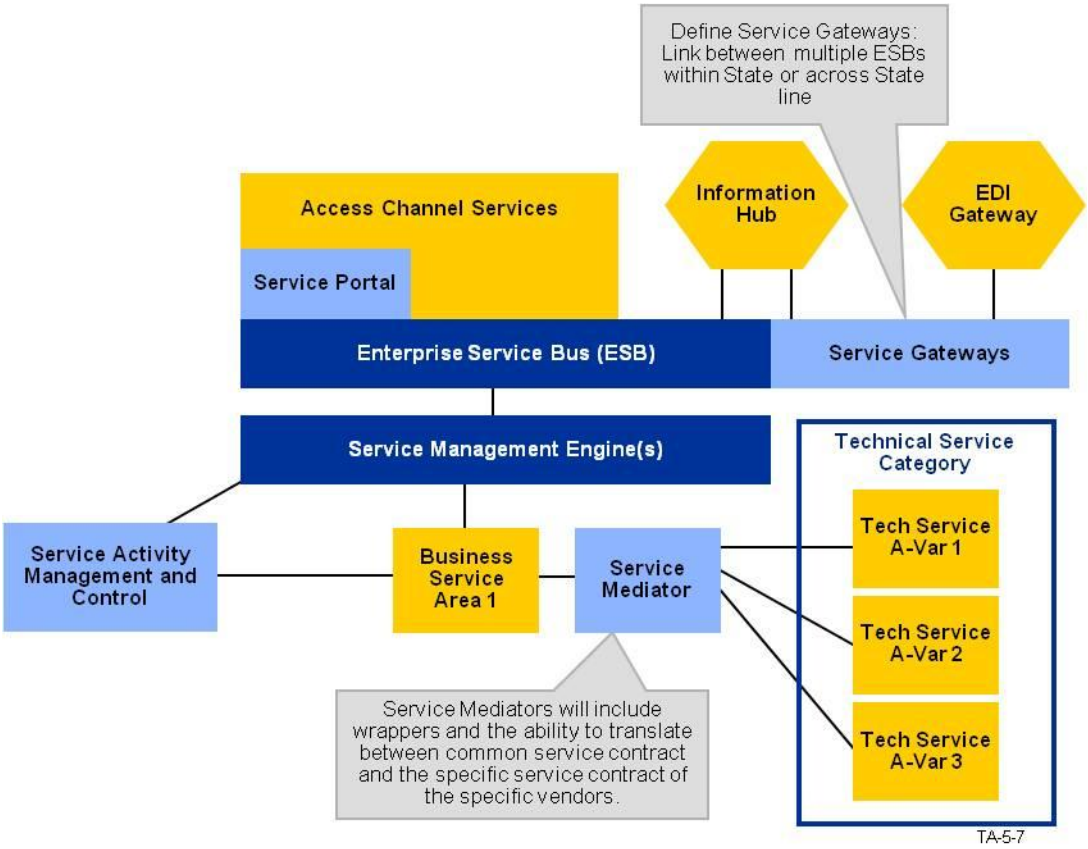
Define Service Gateways: Link between multiple ESBs within State or across State line
Information Hub
EDI Gateway
Access Channel Services
Service Portal
Enterprise Service Bus (ESB)
Service Gateways
Service Management Engine(s)
Technical Service Category
Tech Service A-Var 1
Tech Service A-Var 2
Tech Service A-Var 3
Service Activity Management and Control
Business Service Area 1
Service Mediator
Service Mediators will include wrappers and the ability to translate between common service contract and the specific service contract of the specific vendors.
TA-5-7

Figure 5-8. Service Gateways and Mediators

Distributed Computing and Data Access

As more external private and public sector organizations make solutions to specific requirements available via Cloud Computing, the desire to invoke such services external to the Medicaid Enterprise will increase. Cloud Computing might provide various types of service-oriented solutions on a Software as a Service (SaaS) basis, where stakeholders incur costs only when they invoke a solution. States use a modular, flexible approach to systems development, including the use of open interfaces and exposed APIs. States pursue a service-based and cloud-first strategy for system development. States identify and discuss how they identify, evaluate, and incorporate commercially or publicly available off-the-shelf or open source solutions, and discuss considerations and plans for cloud computing.

Interoperability between the mechanized claims processing and information retrieval systems, eligibility determination systems, and the cloud-based external service(s) may not require any integration through adapters. Other cloud-based external invocations of services or solutions that are not interoperable, including services with non-conforming service contracts, or non-SOA solutions, will likely require some type of data or message transformation as shown in **Figure 5-9** below.

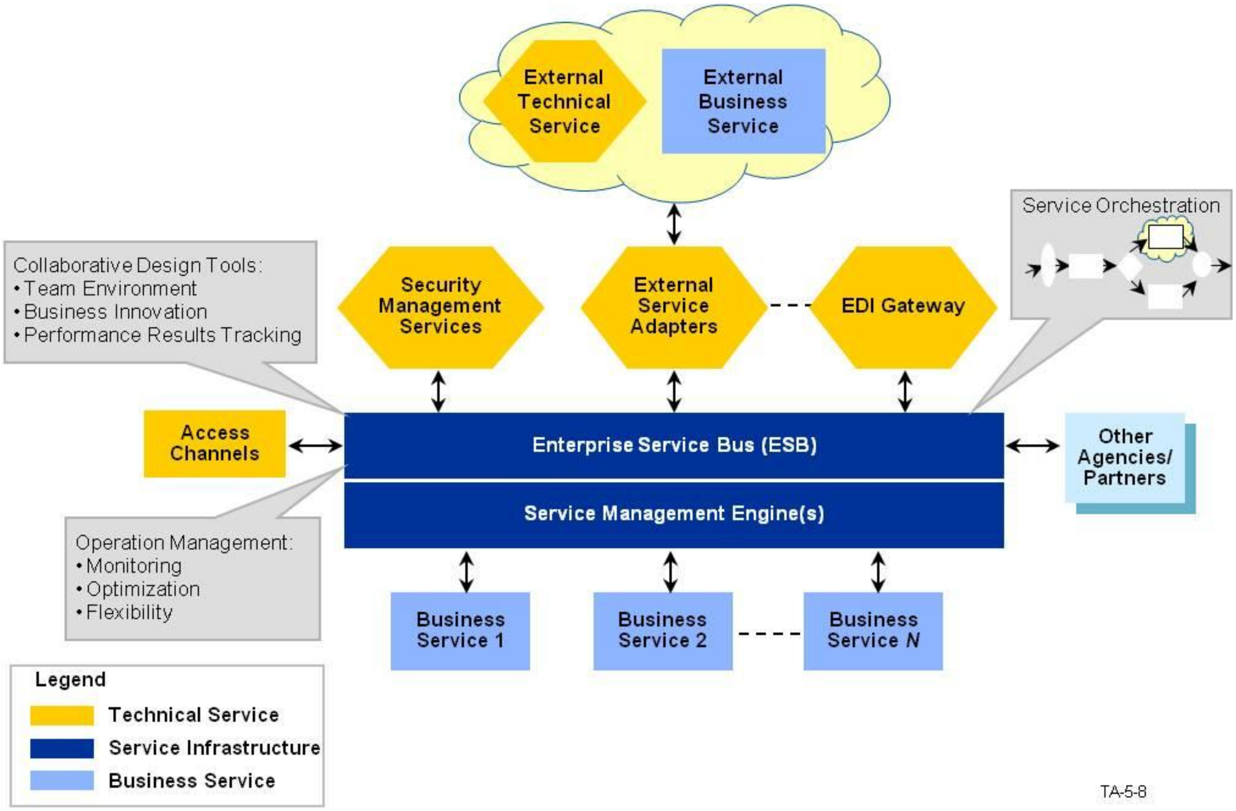

Figure 5-9. Distributed Services via Cloud Computing

The types of services invoked through Cloud Computing are extensive and vary from business services to technical services depending on the need and application. The access to these services, whether based on interoperability or by integration, passes through typical network security frameworks established within the EA.

While external servers perform the processing, the method for accessing external data stores requires a utility service or set of services to connect or transform data. **Figure 5-10** illustrates the orchestration of accessing data residing in a Cloud Computing environment. Query processing, directory management, concurrency control, and deadlock management deals within the Cloud Computing environment by the service provider. Service Level Agreements (SLA) are necessary to cover the numerous coordination and operational details.

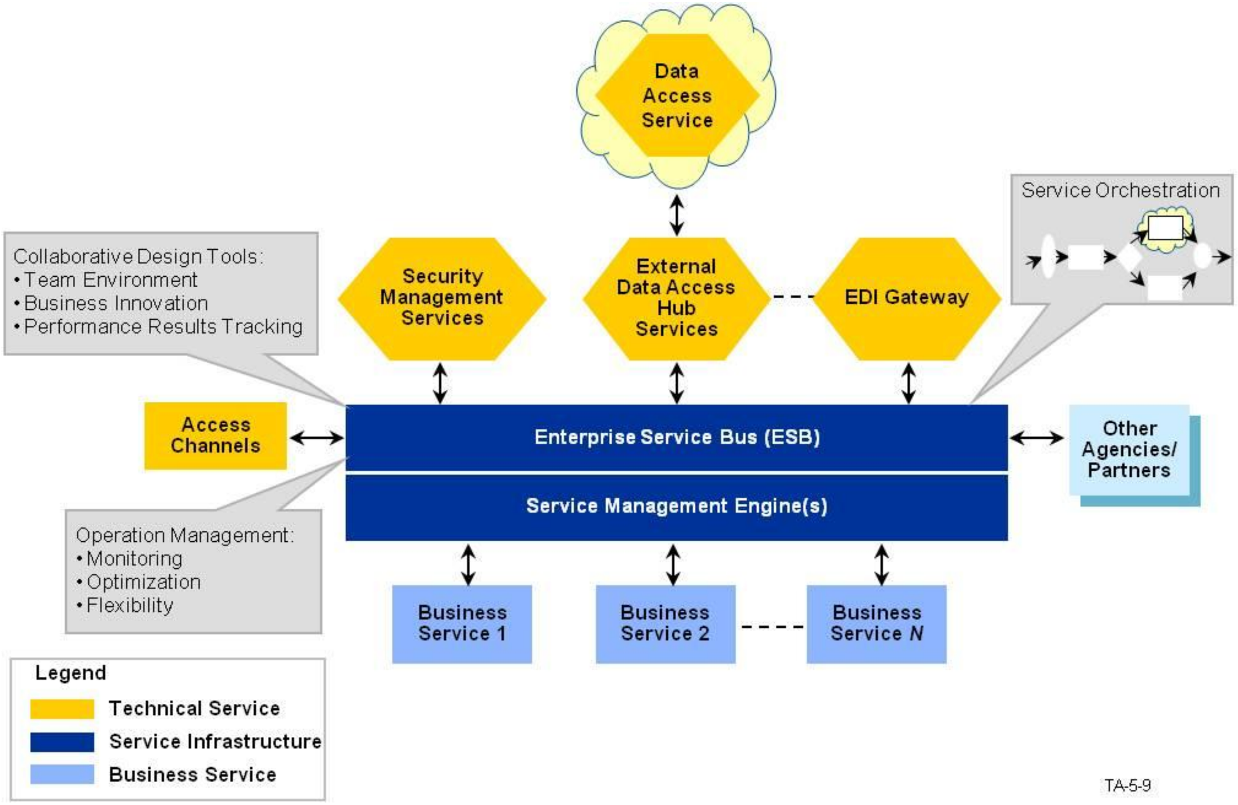

Figure 5-10. Data Access Services via Cloud Computing

Service Interoperability

Interoperability is one of the MITA goals and an overall answer to many of the Medicaid business challenges. Systems must ensure seamless coordination and integration with exchanges (whether run by the state or federal government), and allow interoperability with Health Information Exchanges (HIE), public health agencies, human services programs, and community organizations providing outreach and enrollment assistance services. Technical challenges address business interoperability and include the following:

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

The service-oriented interoperability approach provides technical enablers common ground for addressing key issues, reducing the learning curve, and allowing the Medicaid community to share architecture designs. States can apply hub architecture, interoperability and access channels, and utility services to meet these challenges, as shown in **Figure 5-11.**

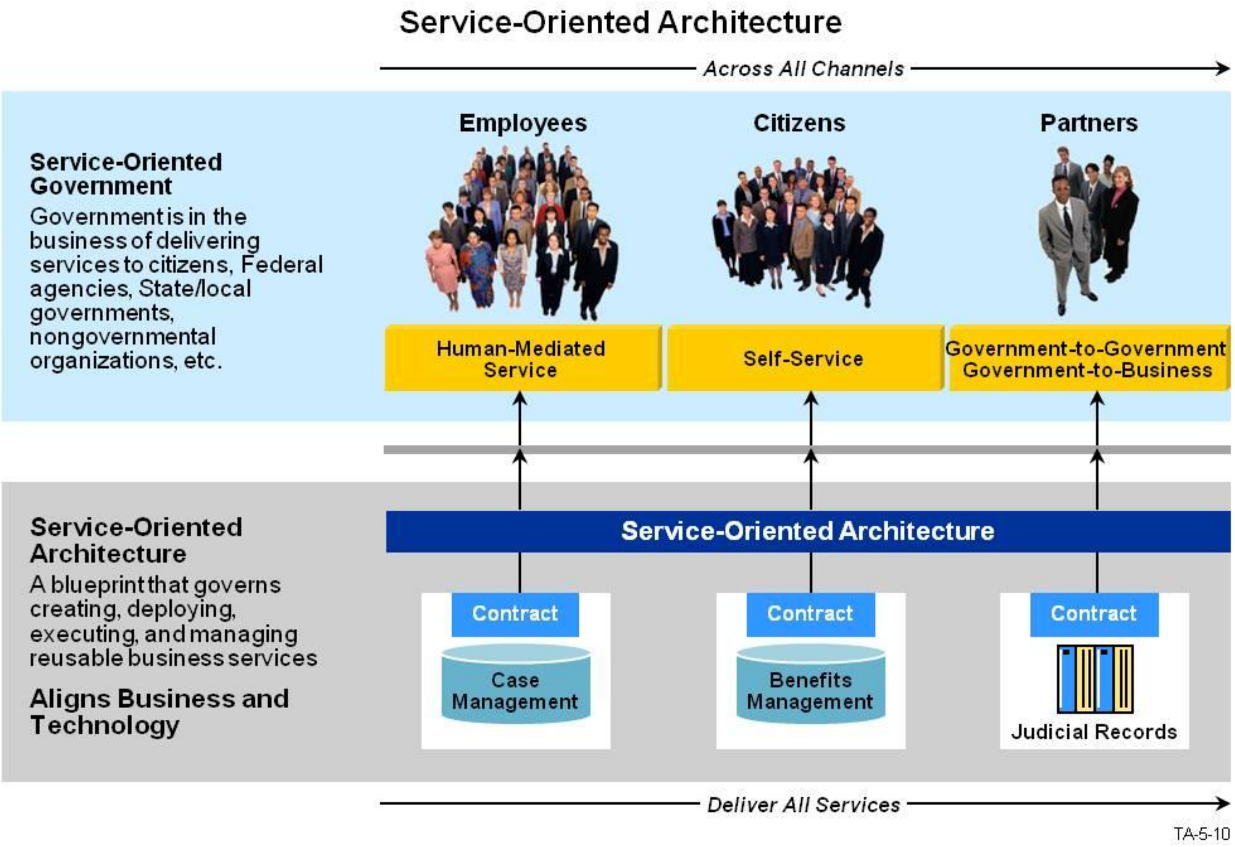
Service-Oriented Architecture
Across All Channels
Employees
Citizens
Partners
Service-Oriented Government
Government is in the business of delivering services to citizens, Federal agencies, State/local governments, nongovernmental organizations, etc.
Human-Mediated Service
Self-Service
Government-to-Government
Government-to-Business
Service-Oriented Architecture
A blueprint that governs creating, deploying, executing, and managing reusable business services
Aligns Business and Technology
Service-Oriented Architecture
Contract
Case Management
Contract
Benefits Management
Contract
Judicial Records
Deliver All Services
TA-5-10

Figure 5-11. Service-Oriented Architecture

KEY SERVICE INTEROPERABILITY ELEMENTS

The crucial concepts for service interoperability are as follows:

- Since interoperability is a by-product of sound programming techniques, it is essential to create SOA-based services following proper design principles with the following characteristics:
  - **Standardized Contract –** Expresses purpose, capability, and interface content quantity.
  - **Loose Coupling –** Defines dependencies between the contract, deployment, and customer.
  - **Abstraction –** Hides as much of the details of the service to preserve loose coupling.

  - **Reusability** – Positions servers as enterprise resources with agnostic function context.
  - **Autonomy** – Designs service logic and deployment of environment impact reliability.
  - **Statelessness** – There is comprised availability when managing excessive Medicaid information.
  - **Discoverability** – Avoids the accidental creation of redundant service or services that implement redundant logic.
  - **Composability** – Complex service compositions place demands on service design.

- 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 recommends 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 separate from applications and design using service utilities.

- Use services to define a logical interoperability architecture (a service overlay) based on hub technology and communication protocols States 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 hide behind interoperability channels and 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 States adapt through variants and extensions. The MITA Framework defines what is common among States, accommodates environmental changes, and provides 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 designed with common underlying architecture and common utility components.

- Define and create virtual access mechanisms that hubs or individual State Medicaid Enterprises can use to exchange information.

ADDITIONAL INTEROPERABILITY DETAIL

The use of hub architectures facilitates the development of interoperable services. A hub architecture differs from data marts and data warehouses in that it does not transfer and store 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. A current day example is the NwHIN.

The Logical Interoperability Model for a hub architecture depicts four (4) types of hubs:

- Service hubs provide external (i.e., distributed) services in a shared data processing manner. Usage of these services requires a detailed SLA to understand the implications of using the service/application (e.g., performance, failure response, data source information).
- Data-sharing coordination hubs store data-sharing agreements and broker the exchange of information among organizations.
- Strategic hubs collect summary information from multiple disciplines. A strategic hub might collect diagnosis information from a Medicaid system and disease information from public health organizations and compare the two data sets.
- Tactical hubs collect information around a specific business area. For example, Medicaid, Medicare, and public health organizations might have tactical hubs that manage data, provider information, and the necessary utilities to collect information about them.

Essential concepts of the Interoperability Model include the following:

- **Interoperability** – Uses common elements and approaches that fit with those of other models and the SMA can adapt to meet its changing needs.
- **Connectors** – Each business area includes business processes and connectors. The type of connection (e.g., asynchronous communication, publish-and-subscribe, and request-and-respond) and the type of information or services exchanged defines the connectors. The Interoperability Model groups topics, subjects, or access to a given type of information 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. Hub architecture is the most mature and offers additional S&P control points that locate utility services on the hub. After the request is at the hub, the utility services accesses information and services through virtual model access.
- **Data model and integration** – Interoperability channels define data translation capabilities in ways that mask incompatibilities.
- **Utility services** – Creates an interoperability channel. An interoperability table defines these elements and allows for adaptations.

- **S&P service components and utilities** –Defined with alternative levels of protection, depending on the services and topics communicated over the channel.
- **Interoperability conflicts** – Identifies interoperability conflicts through interoperability assessments, groups it into business-centric pieces (based on common business interests or purposes), and defines it by interoperability channels.
- **Functionality** – Provides functionality through individualized utility services.

SERVICE INTEROPERABILITY MODELS

The Access Channel Model performs several vital functions:

- Access channels allow state Medicaid staff to access data and information by multiple means (e.g., mobile, wireless, and kiosks) and to interface with organizations that provide batch interaction with messages. Private–Public Partnership Access might include an organization allowed access by its contract. It is essential that the features and functions accessed have clear definitions.
- Access channels protect rights to certain information and allow information sharing through specific interoperability channels. Access channels plan for these exchanges and provide collaborative tools. The access channels and interoperability channels include defined connectors. Connectors define alternate access approaches. Access approaches are adaptable based on policy or failure or recovery conditions.

Table 5-1 provides further details about the Access Channel Model.

Table 5-1. The Access Channel Model

The Access Channel Model	
Question	***Answer***
Importance of the Access Channel Model	The Access Channel Model depicts multiple access channels supported by utility services. Easy data access transforms the Medicaid business. The central concept is the importance of separating access channels from interoperability channels.
Understanding the Access Channel Model	System designers evaluate possible access channels and interoperability channels to make data as readily available as possible.
Using the Access Channel Model	System designers adopt an architecture that separates access channels from interoperability channels and use common utility services to simplify development. These utilities may be available to share within a state, among certain Medicaid systems, or nationally.
Refining the Access Channel Model	The Interoperability Portfolio updates the Access Channel Model. An interoperability portfolio is a collection of services that rely on common definitions and proven SOA characteristics. The portfolio addresses both policy and technical issues regarding the secure data exchange performed by the collection interoperable services.

The Access Channel Model	
Question	***Answer***
Supporting business decisions with the Access Channel Model	New IT procurements adopt the concepts of isolating access and interoperability using utility services.

MITA INTEROPERABILITY MODEL

The use of an ESB provides a valid foundation for TA development. This foundation allows for expansion and is a key component for establishing interoperable application services. The core ESB offering depicted in **Figure 5-12** is a reference throughout this section.

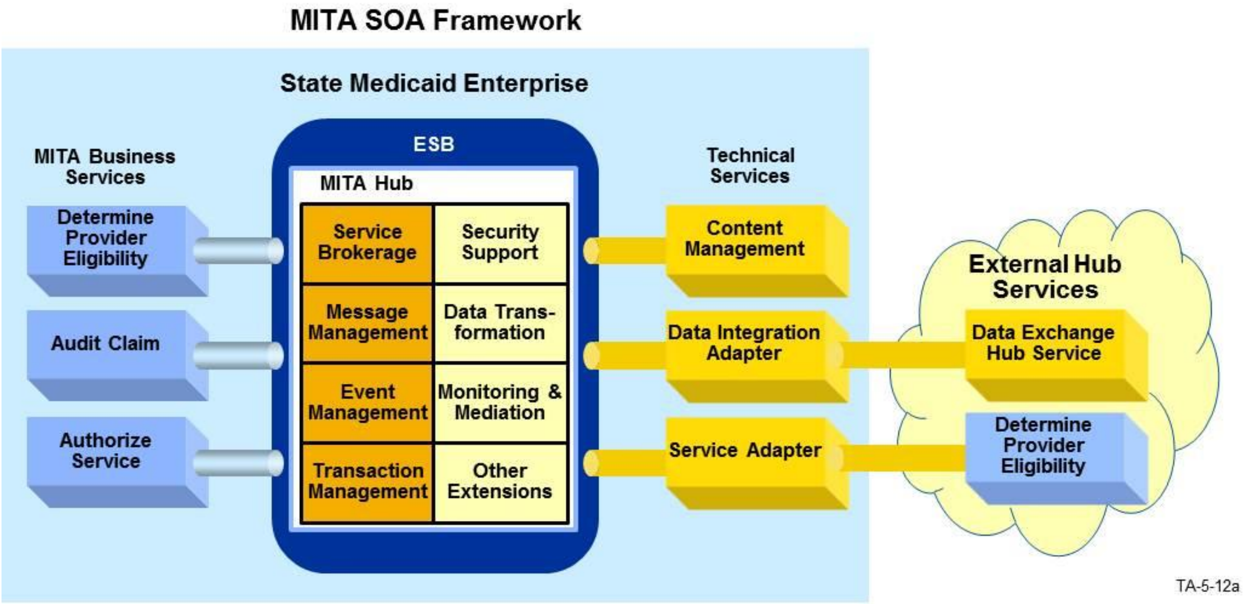

Figure 5-12. MITA SOA Framework ESB Model

The MITA AA has taken a strategic business and technical approach to interoperability, as shown in **Figure 5-13**. The MITA Framework defines interoperability as sub-functions, topics, and types of communication, and understands that conflicts can occur when it uses common solution patterns.

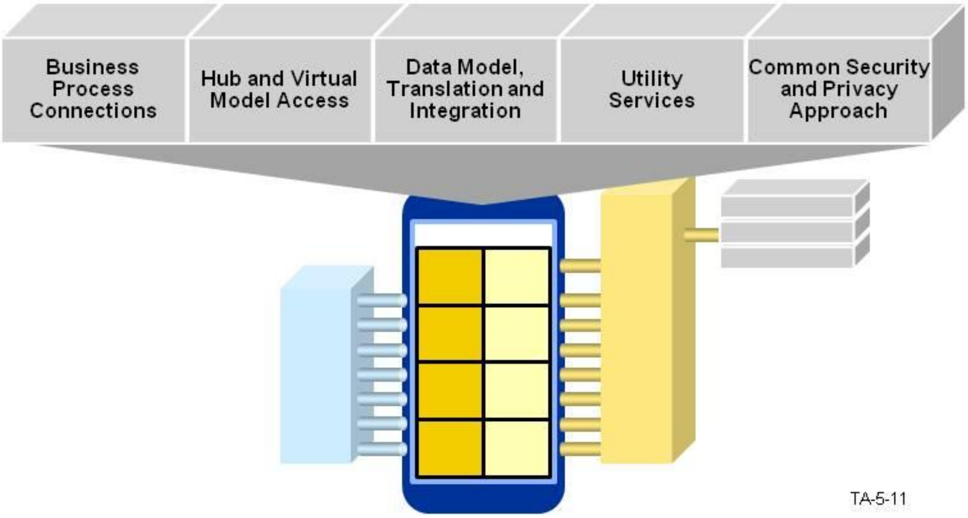
Business Process Connections
Hub and Virtual Model Access
Data Model, Translation and Integration
Utility Services
Common Security and Privacy Approach
TA-5-11

Figure 5-13. Conceptual Interoperability Model

The MITA AA defines separate interoperability channels for each type of information flow and provides the SMA with a definition of utility services shared across the State Medicaid Enterprise. The MITA AA refines interoperability channels collaboratively through the portfolio process.

LOGICAL INTEROPERABILITY LEVEL MODEL

The MITA AA defines and designs its interoperable concepts through a configuration shown in **Figure 5-14.** The MITA Framework defines 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 addresses a minimal set of information sharing needs in a standard way for intrastate data sharing (e.g., with other state departments), among business areas (e.g., storing the data in strategic, tactical data hubs) and with partners (e.g., through the data sharing and coordination hub). The model and concepts extend based on workload as well as the recovery and contingency planning needs.

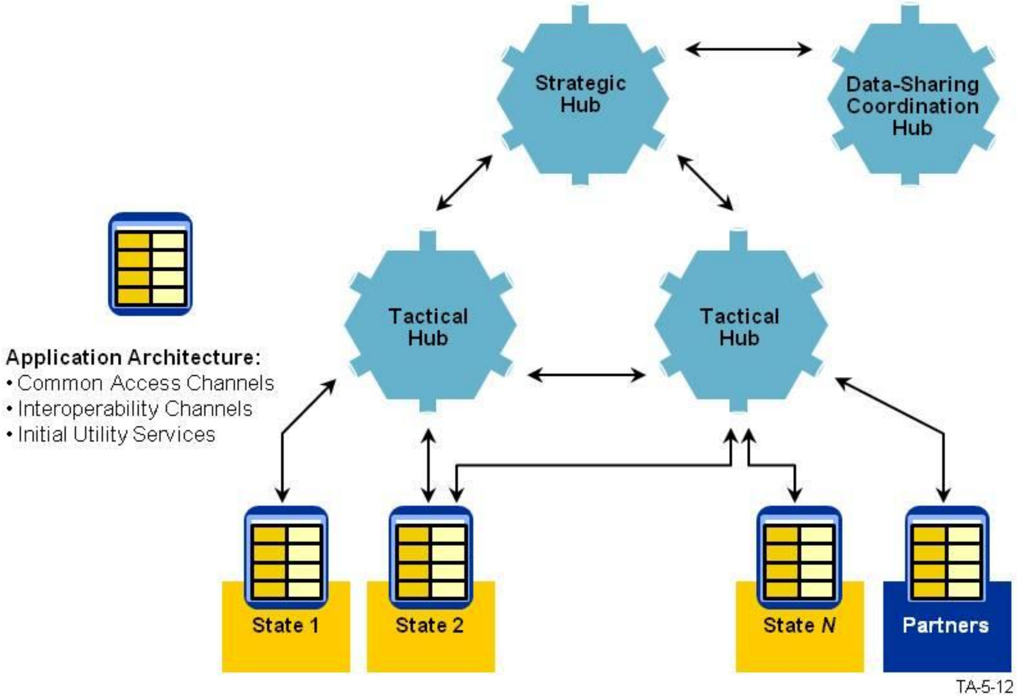
Strategic Hub
Data-Sharing Coordination Hub
Tactical Hub
Tactical Hub
Application Architecture:
• Common Access Channels
• Interoperability Channels
• Initial Utility Services
State 1
State 2
State *N*
Partners
TA-5-12

Figure 5-14. Logical Interoperability Model

Figure 5-14 depicts hub interconnection and illustrates how utility services, the interoperability definition (i.e., configuration files), and security utilities fit together. The significant characteristics are as follows:

- Virtual hubs provide access to data owned and stored by a state and other organizations.
- Common access channels, interoperability channels, and utility services assist data sharing and coordination.
- Partners and States (shown as States 1 – *N*) use a common format. Each state and partner includes utility services and interoperability services functions.
- The four (4) types of hubs are service hubs, 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 hook to the tactical hub.
  - **Service Hub** – This hub hosts the service (i.e., code) that either the calling agent consumes or runs the service on the associated hosted server. An internet-facing hosted server or in a Cloud Computing environment can store this service.
  - **Data-Sharing Coordination Hubs** – This hub gathers and disseminates data based on agreements between partnering organizations. It also links to elements with the NwHIN and other partners, such as the Bureau of the Census or the National Committee on Vital and Health Statistics (NCVHS).

  - **Strategic Hubs** – This hub deals with strategic policy and performance standard capabilities. Stakeholders collect performance and analytical data on an event or periodic basis then send to a data mart configuration with additional related information.
  - **Tactical Hubs** – Two or more tactical hubs support functions that cross state lines or, in cases where data is common, including master reference information, the AA updates and shares with all States to assure consistency.

- 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.

Logical Hub Architecture

As shown in **Figure 5-14** above, States can configure hubs built on standard hub architecture to address tactical, strategic, and data-sharing and coordination functions. The hub architecture consists of three (3) layers:

- **Interface Management Layer**
  - 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.
  - Supports the adaptability needs or any necessary manual functions, such as special queries.
- **Data Management Layer** – Houses data stores that are either data marts or relational data models. It also includes a virtual data access capability.
- **Utility Services Layer** – Represents the portions of utility services that reside on the hub or server (often called the *servlet*) and provides capabilities to run on the hub, such as access to virtual models, collection, filtering, and delivery of blocks of information to the business area.

Table 5-2 outlines the reasons for using an Interoperability model.

Table 5-2. The Interoperability Model

The Interoperability Model	
Question	***Answer***
Importance of the Interoperability Model	The Interoperability Model describes the business capabilities and technical functionality necessary to achieve efficient system-to-system interactions.
Understanding the	System designers understand the concepts in the Interoperability

The Interoperability Model	
Question	***Answer***
Interoperability Model	Model and incorporate them into system designs.
Using the Interoperability Model	The Interoperability Model provides guidance and recommendations that support the design and development of services and data that the Medicaid community can share, although the SMA retains its autonomy. The SMA can follow the model to achieve cross-organizational information sharing through a common approach.
Refining the Interoperability Model	The Interoperability Portfolio updates the Interoperability Model. An interoperability portfolio is a collection of services that rely on common definitions and proven SOA characteristics. The portfolio addresses both policy and technical issues regarding the secure data exchange performed by the collection of interoperable services.
Supporting business decisions with the Interoperability Model	New IT procurements adopt these concepts of interoperability.

Leveraging Interoperability Projects

- Intelligence agencies have an extensive infrastructure that links several business areas.
- These projects address federal-to-state communications, such as communications that involve the Centers for Disease Control (CDC), the Internal Revenue Service (IRS) (e.g., tax or child support liens), 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 architectural alignment the Federal Chief Information Officers Council is pursuing with the Office of Management and Budget's Federal Enterprise Architecture Program Management Office (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.

Security and Privacy

Security and Privacy (S&P) are critical to the Medicaid Enterprise. The MITA Framework 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. S&P crosscuts all design aspects with a limited group of common centralized elements that may have many distributed mechanisms and controls. Established role-based standards achieve a fundamental mechanism for privacy of data. These role-based security functions provide the access management means in a repeatable and auditable manner in a routine fashion.

Terminology and Concepts

This section provides descriptions of common S&P terms and concepts.

- **Authentication** - To positively verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system.
- **Authorization** – Governs the resources and operations that the authenticated client is able to access. Resources include files, databases, tables, and rows, as well as other enterprise resources (e.g., registry key and configuration data). Operations include performing transactions such as enrolling a provider, transferring a member from one provider account to another, or prior approval (i.e., prior authorization).
- **Auditing** – Effective auditing and logging is important 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 variation might be refusing to perform a surgery after the audit trail shows that the provider approved it.
- **Confidentiality** – Confidentiality means ensuring data remains private and 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 (ACL), where the state staff handles personal medical information by following certain privacy procedures discussed in more detail below.
- **Integrity** – Integrity is a guarantee that the SMA protects data from accidental or deliberate (i.e., malicious) modification. Like privacy, integrity is a major 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** – Means the system remains available to legitimate users. Some attackers, such as those the SMA denied service, may seek to crash an application or overwhelm it so other users cannot access it.
- **Asset** – A resource of value, such as data in a database or a system resource.
- **Threat** – A potential occurrence (malicious or otherwise) that might harm an asset.
- **Vulnerability** – A weakness that makes a threat possible.
- **Attack (or Exploit)** – An action taken to harm an asset.
- **Countermeasure** – A safeguard that addresses a threat and mitigates risk.

Security and Privacy Focuses

The SMA integrates features of S&P throughout the State Medicaid Enterprise, including legislative and policy goals, supported by a risk management approach. The discovery of the S&P business needs is often a neglected activity. Some organizations have attempted to add-on S&P features; however, this is both difficult and problematic, as experience with HIPAA has shown.

S&P also includes a business perspective that: brings issues to the attention of all involved with the State Medicaid Enterprise; weaves S&P considerations into all aspects of the business process; and incorporates each new business initiative and each change in technology. Although S&P is complex management, business leaders, partners, and customers of the services delivered need to take into account their differing levels of understanding and needs. It is essential that citizens who receive services and supply personal data trust the SMA ability to secure and protect their information. Organization leaders need to have a commitment to protect valued assets and maintain continuity of services.

The MITA Framework considers 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 the MITA AA leverages in its S&P business impact analysis. The business modeling approach utilizes business use cases. To integrate S&P into business models, the SMA will extend business use cases with S&P-specific information.

An example S&P use case would 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 service denial, computer viruses or worms, and defacing of a website or portal. Additional privacy concerns include the inadvertent release and modification of personal data, violation of usage agreements, or health crisis override of privacy preferences.

S&P mechanisms integrate into the business and technical models. S&P activities are crosscutting activities that define protection mechanisms, components, operations processes, as well as roles and responsibilities. Stakeholders factor the S&P business principle into all services and models. This business principle addresses the following:

1. **Providing Protection with Low Maintenance –** 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.
2. **Consistency Across Medicaid –** To provide a base for the Medicaid community and align with initiatives such as the FHA and the NwHIN as they address S&P. The MITA Framework also addresses common issues as seen from other industries. A consistent

approach allows 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 Health Care Industry.

3. **Role Based Access Controls –** To establish defined user security profiles based on roles within the Medicaid Enterprise. This proven method provides a sound privacy foundation that surrounding applications can leverage.
4. **Adaptability and Responsiveness –** To adequately respond to new threats and viruses and to the new technologies that counter them, the MITA Framework adapts and extends S&P features as the IT and Health Care Industries identifies new threats and new forms of attack.
5. **Platform/Software Independence –** To meet vital principles that transcend development technology and application scenarios, S&P models simultaneously meet policy needs using the best available technologies within the resources.
6. **Cross-Agency Integration and Alignment** – To align across the enterprise with a set of controlled and managed interfaces that follow a set of policies, S&P risks 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.
7. **Going Beyond HIPAA** – To provide a S&P solution set, the SMA implements the Health Insurance Exchange (HIX) and the Health Information Exchange (HIE) to tie infrastructures together.
8. **Defining Goals and Objectives –** To provide formal policies based on industry-standard S&P language that the SMA can access and share, with security service elements in packages and in a unified but distributed and federated S&P framework.

Basic Approach

S&P ties to the AA in the Medicaid Enterprise and, to some extent, to cross-government activities. This approach is parallel with the efforts of NASCIO, participants from the National Institute of Standards and Technology (NIST), and other industry associations. The MITA Framework does the following:

- Explains the drivers for S&P and HIPAA S&P rules that the SMA understands and is actively working on.
- Leverages the activity of upgrading NIST guidance based on E-Government 2002 directives.
- Develops a risk and value management approach that combines experience with Federal Information Security Management Act (FISMA) reporting activities.
- Defines an approach that balances short-term reaction (often occurs with a new virus or security breach) with longer-term activities to integrate S&P.
- Defines a process to build services and solution mechanisms into all portions of the architecture and link them to standards and commercial products.

- Leverages 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 Health Care Industry and of other industries (e.g., health insurance) to adopt and influence S&P standards.
- Utilizes the following documents for background and reference:
  - NIST documents
  - HIPAA S&P rules
  - CMS reports
  - Department of Health and Human Services (HHS) guidance
  - NASCIO guidance

Table 5-3. Basic MITA S&P Principles

Basic MITA S&P Principles	
Principle	***Concepts***
Compartmentalize	Reduce the surface area of attack. Ask how the SMA will contain a problem. If an attacker takes over an application, what resources can the attacker access? Can attacker access network resources? How is the SMA restricting potential damage (e.g., firewalls, least privileged accounts, and least privileged code)?
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	Defense in depth means that SMA does not rely on a single layer of security and assume that individuals may bypass or comprise one of the layers. Use multiple gatekeepers to keep attackers at bay. Can the SMA survive if one firewall between different zones is not operational?
Do not trust user input	An application's user input is the attacker's primary weapon when targeting an application. Assume all input is malicious until proven otherwise and apply an in-depth strategy to validate input; taking particular care to ensure the system validates input whenever a user crosses a trust boundary in an application.
Check at the gate	Authenticate and authorize callers early – at the first gate, and reauthorize periodically.
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 attacker exploit vulnerabilities in your application.

Basic MITA S&P Principles	
Principle	***Concepts***
Secure the weakest link	Is there vulnerability at the network layer an attacker can exploit? What about other points?
Create secure defaults	Is the default account set up with least privilege? Does the SMA disable the default account by default and then explicitly enable it 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 the client can use against the system?
Reduce your attack surface	If the SMA is not using the feature or function, disable it. Reduce the surface area of attack by disabling or removing unused services, protocols, and functionality. Does the server need all those services and ports? Does the application need all these features?

CONCEPT MAPS

The MITA Framework uses the concept map as a navigation tool for the many tools, standards, models, and actions States take to integrate S&P into all the elements of their enterprises, with special focus on the cross-enterprise data sharing and shared services. **Figures 5-15**, **5-16**, and **5-17** present the concept maps below.

BASIC PRINCIPLES

Stakeholders align EA and S&P architecture with changes necessary to harden and strengthen the protections as shown in **Figure 5-15.**

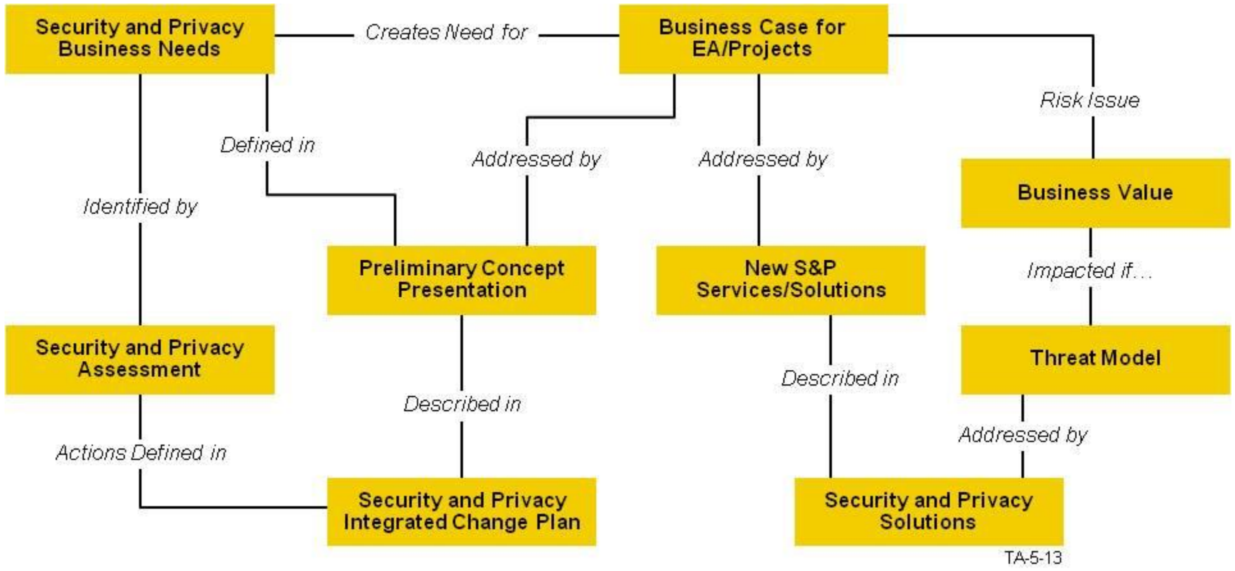
Security and Privacy Business Needs
Creates Need for
Business Case for EA/Projects
Risk Issue
Defined in
Addressed by
Addressed by
Business Value
Identified by
Preliminary Concept Presentation
New S&P Services/Solutions
Impacted if...
Security and Privacy Assessment
Threat Model
Described in
Described in
Addressed by
Actions Defined in
Security and Privacy Integrated Change Plan
Security and Privacy Solutions
TA-5-13

Figure 5-15. Aligning S&P and Enterprise Architecture

INTEGRATE SECURITY AND PRIVACY INTO ENTERPRISE ARCHITECTURE

The second concept map depicts the steps necessary to integrate S&P into the strategy, EA, and into other related solution sets as shown in **Figure 5-16.**

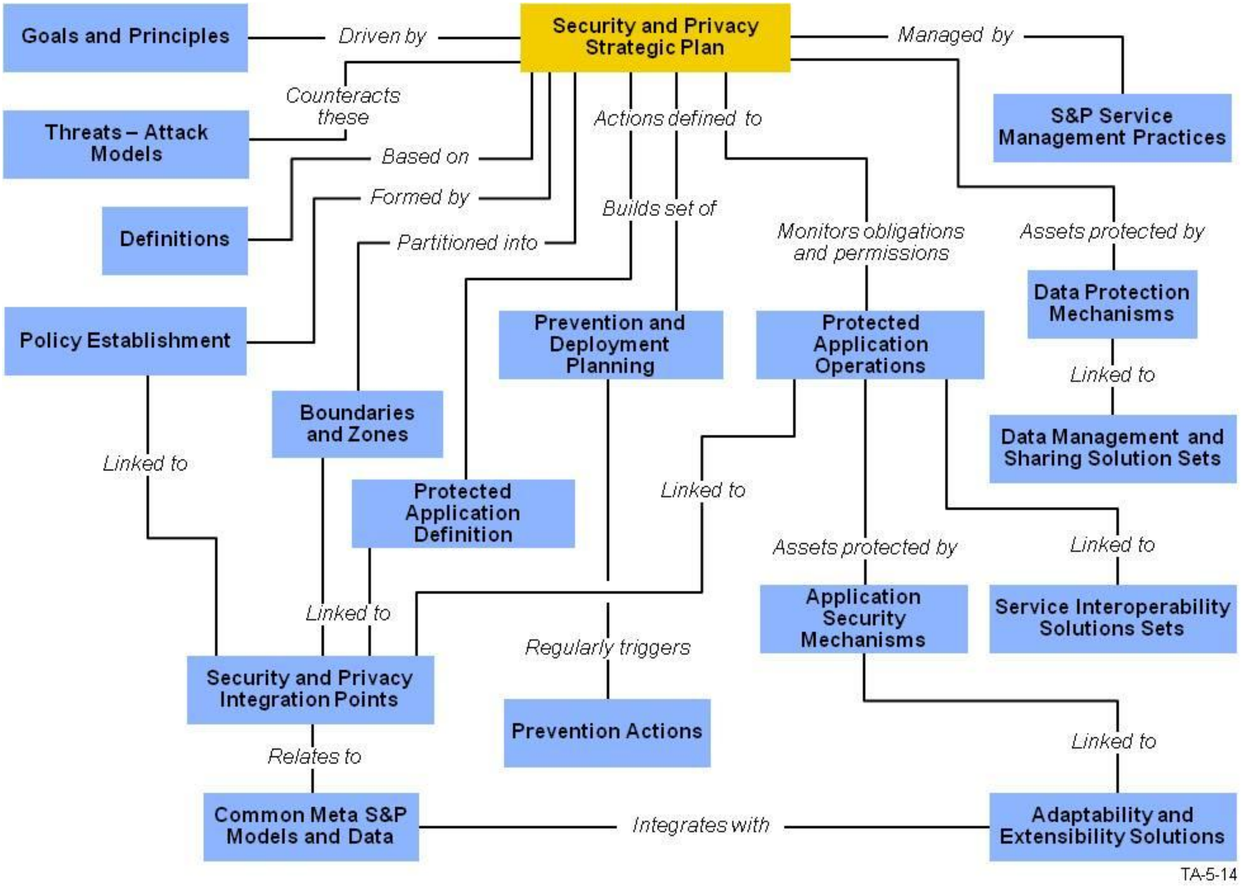
Goals and Principles
Driven by
Security and Privacy Strategic Plan
Managed by
Threats – Attack Models
Counteracts these
S&P Service Management Practices
Actions defined to
Based on
Definitions
Formed by
Builds set of
Partitioned into
Monitors obligations and permissions
Assets protected by
Data Protection Mechanisms
Policy Establishment
Prevention and Deployment Planning
Protected Application Operations
Linked to
Boundaries and Zones
Data Management and Sharing Solution Sets
Linked to
Protected Application Definition
Linked to
Assets protected by
Linked to
Application Security Mechanisms
Service Interoperability Solutions Sets
Linked to
Regularly triggers
Security and Privacy Integration Points
Prevention Actions
Relates to
Linked to
Common Meta S&P Models and Data
Integrates with
Adaptability and Extensibility Solutions
TA-5-14

Figure 5-16. Aligning S&P and Strategy Architecture

SECURITY AND PRIVACY ELEMENTS

The third concept map describes the S&P elements and their links as shown in **Figure 5-17.**

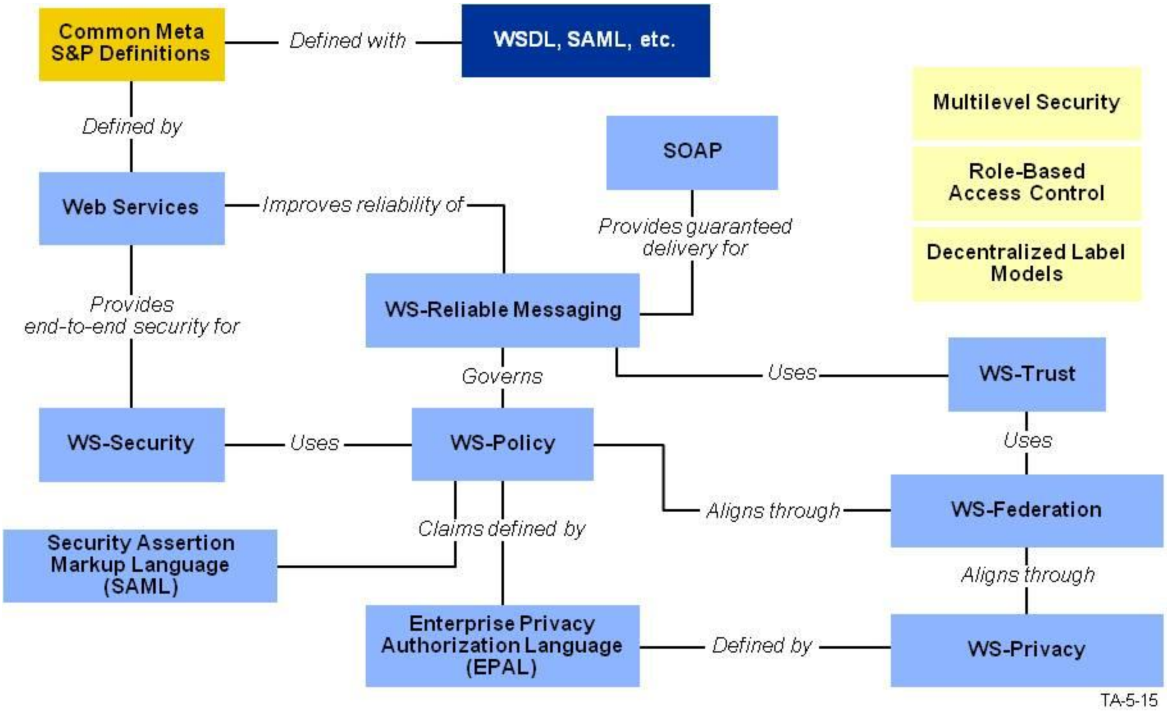

Figure 5-17. MITA S&P Standards

Application Architecture Framework

The MITA AA defines a crosscutting extended enterprise and layered approach and maps it to S&P standards with known gaps. The framework, shown in **Figure 5-18** originates from the Objective, Model, Architecture, and Mechanism (OM-AM) Framework developed by Park and Sandhu from George Mason University.

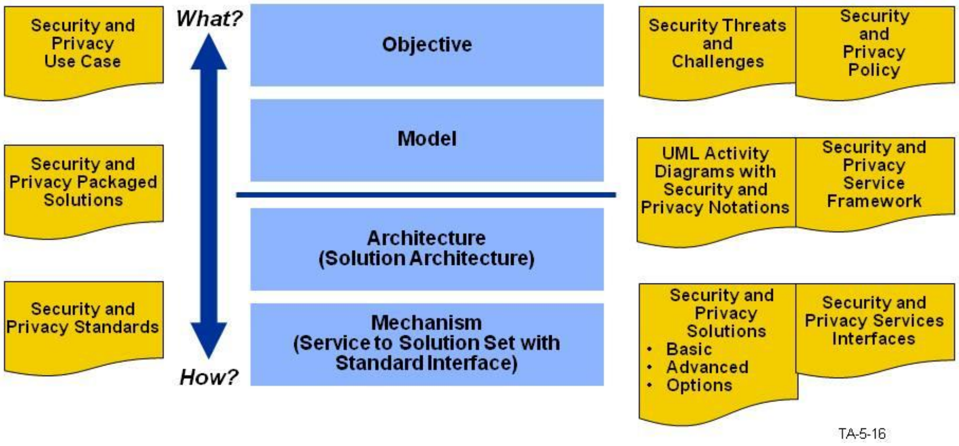
Security and Privacy Use Case
Security and Privacy Packaged Solutions
Security and Privacy Standards
What?
How?
Objective
Model
Architecture (Solution Architecture)
Mechanism (Service to Solution Set with Standard Interface)
Security Threats and Challenges
Security and Privacy Policy
UML Activity Diagrams with Security and Privacy Notations
Security and Privacy Service Framework
Security and Privacy Solutions
• Basic
• Advanced
• Options
Security and Privacy Services Interfaces
TA-5-16

Figure 5-18. S&P and the OM-AM Model

Objective and Model layers articulate the security objectives. Architecture and Mechanism describe how to achieve them. Within the OM-AM Framework, each layer maps to the adjacent layers in many ways. For example, an RBAC model is very popular as is a Desired Configuration Management (DCM) (also referred to as Settings Management) but different products deploy in different ways. For example, the RBAC model provides a well-understood way of discussing roles and responsibilities; mapping them to processes to ensure the same person can both authorize and receive information. The DCM defines how to manage data and documents, controlling access to those documents.

SECURITY THREAT MODELS

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 chain that have goals. One can describe threats based on the purpose of the attack. Each service analysis includes defining the use and the types of services provided by one or more endpoint resource along the defined channel. The threat model began 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 organizes threat categories around Microsoft's STRIDE Threat Model. STRIDE originates from an acronym for the following six (6) threat categories:

- **Spoofing** –Attempting to gain access to a system by using a false identity. Attackers can accomplish this 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** – Unauthorized modification of data (e.g., as it flows over a network between two computers).

- **Repudiation** – The ability of users (legitimate or otherwise) to deny they performed a specific action or transaction. Without adequate auditing, repudiation attacks are difficult to prove.

- **Information Disclosure –** The unwanted exposure of private data (e.g., a user viewing data that the user has no authorization 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 –**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 that can crash an application process.
- **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.

The industry has adapted the Service Threat Modeling Process from the Microsoft process with extensions and integration with the service value chain analysis activities and role engineering and multi-attribute decision criteria. The key construct is the service diagram that defines the services used and those provided by the systems and people 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 automatic except for exception processing. The service delivery architecture defines the business process involved in delivering these services, since the composition of these business services into composite services known as service contexts can introduce additional threats.

A service context may be for employees performing different roles, or the contexts for the customer, citizen, or member 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 exists, 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:
   A. How much damage can be done if someone exploited the vulnerability? (Damage Potential)
   B. How easily can someone reproduce the attack? (Reproducibility)
   C. How easily can someone launch an attack? (Exploitability)

   D. Approximately how many users does it affect? (Affected Users)
   E. How easily can someone find the vulnerability? (Discoverability)
7. Perform multi-criteria countermeasure analysis.
8. Summarize residual threats.

The IT and Health Care Industries make S&P decisions based on threat-driven scenarios, associated impact, and value assessments.

SECURITY AND PRIVACY MODEL

The MITA team provides the S&P Goals and Policy Model, shown in **Figure 5-19** based on security goals and policies from various federal government documents.

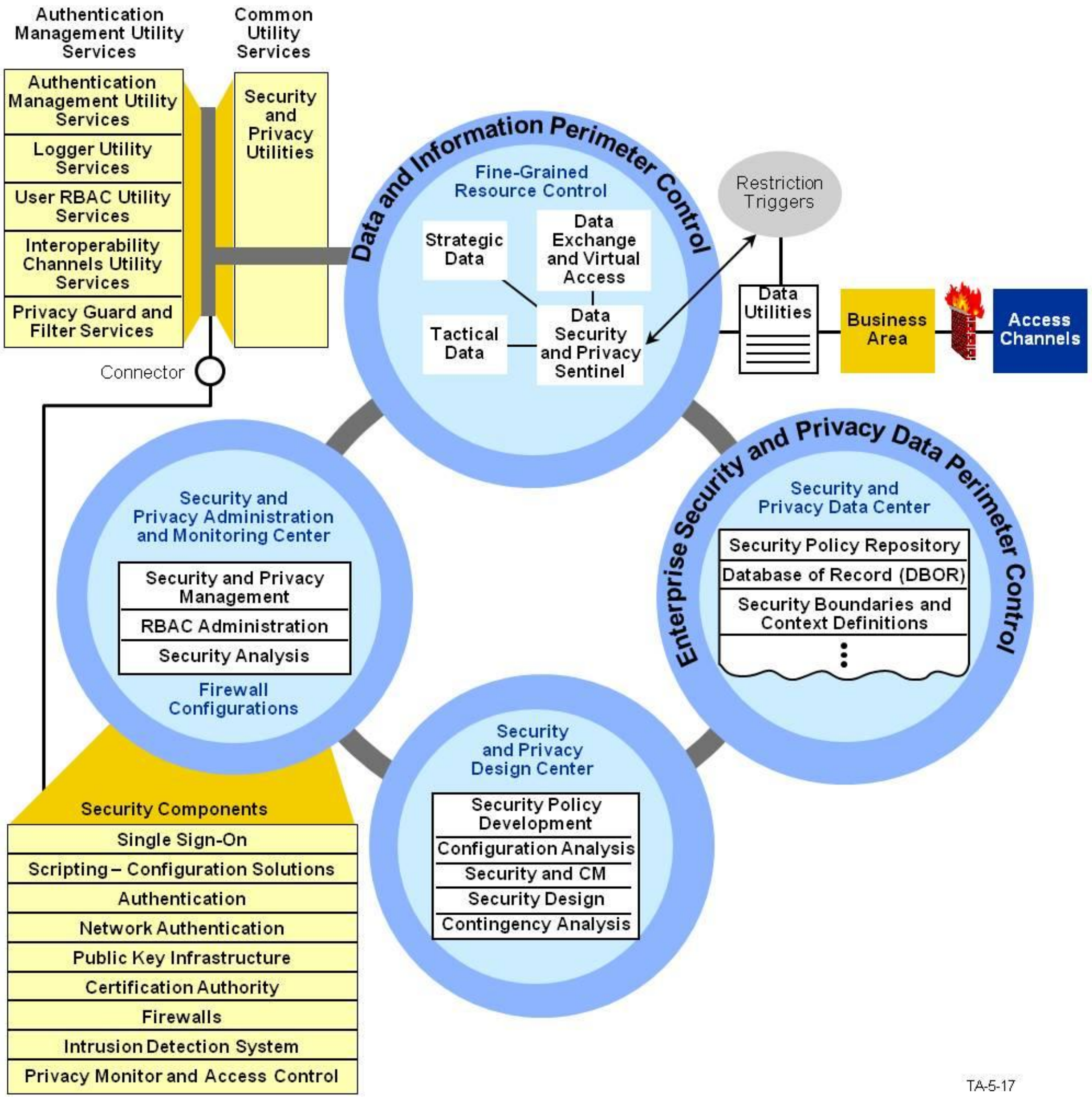
Authentication Management Utility Services
Common Utility Services
Authentication Management Utility Services
Logger Utility Services
User RBAC Utility Services
Interoperability Channels Utility Services
Privacy Guard and Filter Services
Security and Privacy Utilities
Connector
Data and Information Perimeter Control
Fine-Grained Resource Control
Strategic Data
Data Exchange and Virtual Access
Tactical Data
Data Security and Privacy Sentinel
Restriction Triggers
Data Utilities
Business Area
Access Channels
Enterprise Security and Privacy Data Perimeter Control
Security and Privacy Data Center
Security Policy Repository
Database of Record (DBOR)
Security Boundaries and Context Definitions
Security and Privacy Administration and Monitoring Center
Security and Privacy Management
RBAC Administration
Security Analysis
Firewall Configurations
Security and Privacy Design Center
Security Policy Development
Configuration Analysis
Security and CM
Security Design
Contingency Analysis
Security Components
Single Sign-On
Scripting – Configuration Solutions
Authentication
Network Authentication
Public Key Infrastructure
Certification Authority
Firewalls
Intrusion Detection System
Privacy Monitor and Access Control
TA-5-17

Figure 5-19. Security and Privacy Goals and Policies

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

Four (4) 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 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.

The MITA AA describes packaging security capabilities in the form of COTS components that the SMA may adapt based on its policies and configurations. Those S&P components integrate into the business and technical models at the S&P connection points. The defined security components link with S&P utility services the SMA integrates with its business area processes and related components.

S&P components include the following:

- **Single Sign-On** – Ability to sign on to an enterprise 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** – Ability to determine the authenticity of a person who seeks access to tactical, strategic, or data sharing hubs (e.g., through Public Key Infrastructure (PKI), Certification Authority, or Registration Authority).
- **Network Authentication –** Ability to control interoperability channels and protect interstate and national communications.
- **Firewalls** – Dynamically configured.
- **Intrusion Detection System** – Ability to detect and flag behaviors that might indicate a security threat or violation.
- **Privacy Monitor and Access Control** – Ability to protect private data and log and report any disclosure.

The MITA AA describes S&P utilities that bridge business areas and S&P components. **Table 5-4** below depicts the initial set of S&P utility services and features and the connections to the related components.

Table 5-4. Security and Privacy Related Components

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, 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. Provides controls that can increase or decrease logging levels.	S&P data center receives logging information.	Audit system
User RBAC Utility Services	Connects roles to business areas, users who requested services, and context the user works in.	S&P defines constraints based on separation of responsibilities (a crucial area the SMA adapts as it adds and changes staff).	S&P Data Center
Interoperability Channels Utility Services	Each interoperability channel and access channel has rights of access defined. These functions map to the RBAC utilities.	Utilities can detect mismatches of rights and report potential threats. Ability to reconfigure and change the interoperability channel definition files.	Firewalls Intrusion and Detection Center
Privacy Guard and Filter Services	Certain data and information has 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 (3) components:

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

The MITA team separated these functions in order to protect and provide a coordinated use of multiple security countermeasures to protect the integrity of the information assets in an enterprise strategy with separate firewalls used for each. The critical resource is the data and the S&P information about the data.

Data and Information Security uses fine-grained security labels with the data hubs and include special resource access triggers that integrate with utility services.

Concerns and Challenges

CONCERNS

The cross-organization nature of the data and services shared among the Medicaid and other health care communities raises several critical issues the MITA AA is addressing with specific best-for-now approaches that appear in modules and are subject to change. 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.
    - Authorize sharing of new data container.
- Security standards framework
    - Policy Layer: Web Service (WS)-Policy, WS-Trust, WS-Privacy, Security Assertion Markup Language (SAML), Enterprise Privacy Authorization Language (EPAL)
    - Federation Layer: WS-Secure Conversation, 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

It is necessary for S&P to integrate throughout the architecture. It is important that S&P experts understand and support the mission and business goals of the Medicaid Enterprise and MITA initiative.

Some of the significant challenges include:

- **Inconsistent or nonexistent guidance** – NIST guidance is not consistent with e-government transformation needs.
- **Complexity** – S&P technology is complex and multilayered, TA needs to integrate it from the beginning.
- **Threats** – S&P addresses new threats immediately and yet accommodates new and changing technologies (e.g., WS), while promoting security infrastructure reuse.
- **Enterprise Security Perspective** – Migration from a system perspective to an enterprise perspective includes 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-driven critical processes. Architects and designers define the data, map it to other subject data models, and protect it. **Figure 5-20** depicts the Enterprise S&P Data and Information Subject Area Model.

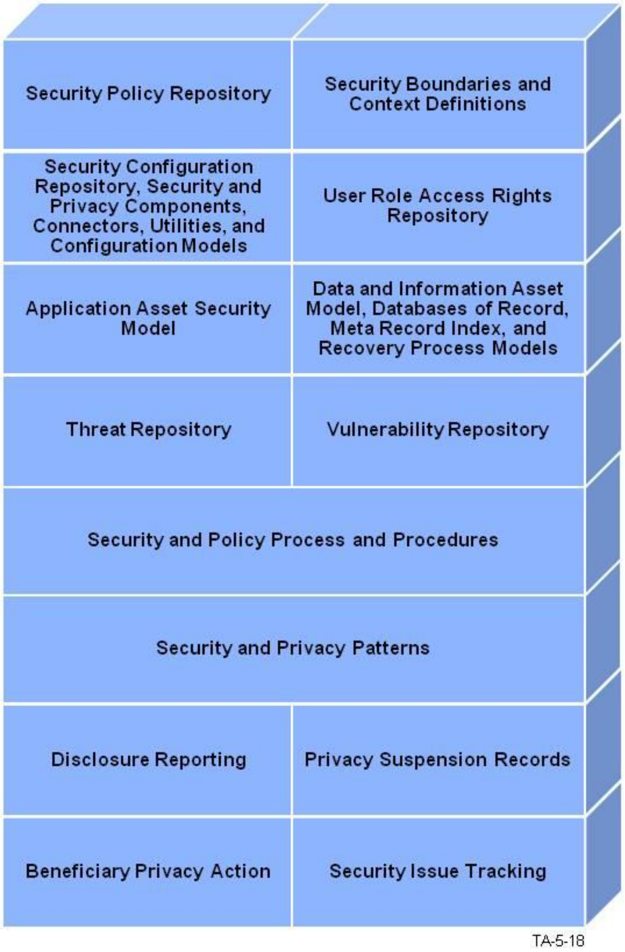
Security Policy Repository
Security Boundaries and Context Definitions
Security Configuration Repository, Security and Privacy Components, Connectors, Utilities, and Configuration Models
User Role Access Rights Repository
Application Asset Security Model
Data and Information Asset Model, Databases of Record, Meta Record Index, and Recovery Process Models
Threat Repository
Vulnerability Repository
Security and Policy Process and Procedures
Security and Privacy Patterns
Disclosure Reporting
Privacy Suspension Records
Beneficiary Privacy Action
Security Issue Tracking
TA-5-18

Figure 5-20. Security and Privacy Data and Information Subject Area Components

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

- An S&P policy repository defines the agreed-on S&P policies, using an English language agreement and declarative S&P policy languages (e.g., SAML).
- Definitions for S&P boundaries or zones also include any established Demilitarized Zone (DMZ) or firewall areas.
- Security configuration repository elements, including security components that map security patterns to vendor products and security capabilities offered. An application asset repository that includes an S&P template assessment to identify risks for each business area and portion of a business area.
- A threat repository captures information about known attacks the architecture addresses and other threats that S&P considers.

- A vulnerability repository includes computer vulnerability evaluation forms classified based on security standards and mapped to the MITA business and technical models.
- S&P patterns and icons the MITA AA defines using a common pattern template.
- Summary S&P notification and guidance is open to all and based on an ongoing communication effort. S&P is an important part of the State Medicaid Enterprise and ongoing operations. One of the announcements is a roles-and-responsibilities notification, including to specialists, on certain security components (e.g., firewalls, intrusion detections, and directories).

SECURITY LEVELS

For each major element of security, TA defines three (3) levels of S&P as follows:

- 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 coordinates the refinement of these models and the establishment of the capabilities needed for each level, as discussed in **Table 5-5.**

Table 5-5. Security and Privacy Model

Security and Privacy Model	
Question	***Answer***
Importance of the S&P Model	The S&P model depicts a consistent way of designing security across the network. Essential concepts are single sign-on/log-in, use of standards, and a wide range of security components.
Understanding the S&P Model	System designers review the model to ensure it has addressed all appropriate levels of security.
Using the S&P Model	The S&P model offers many design options. System designers select components appropriate for data sharing and access requirements to meet business needs.
Refining the S&P Model	The S&P Portfolio team updates the S&P model.

Security and Privacy Model	
Question	***Answer***
Supporting business decisions with an S&P Model	New IT procurements specify the appropriate security components to support data sharing.

Services and Infrastructure Interaction

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

Adding a Service

The SMA conducts the following six (6) steps to add a new service to its infrastructure, as shown in **Figure 5-21.**

1. **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 intrastate agencies or between a state agency and another organization that involves a business area. For example a state agreement with CMS on Medicaid, with the CDC on vaccines, or with the Food and Drug Administration (FDA) on adverse drug event reporting. The MITA Framework provides the SMA with a business interoperability agreement format 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.

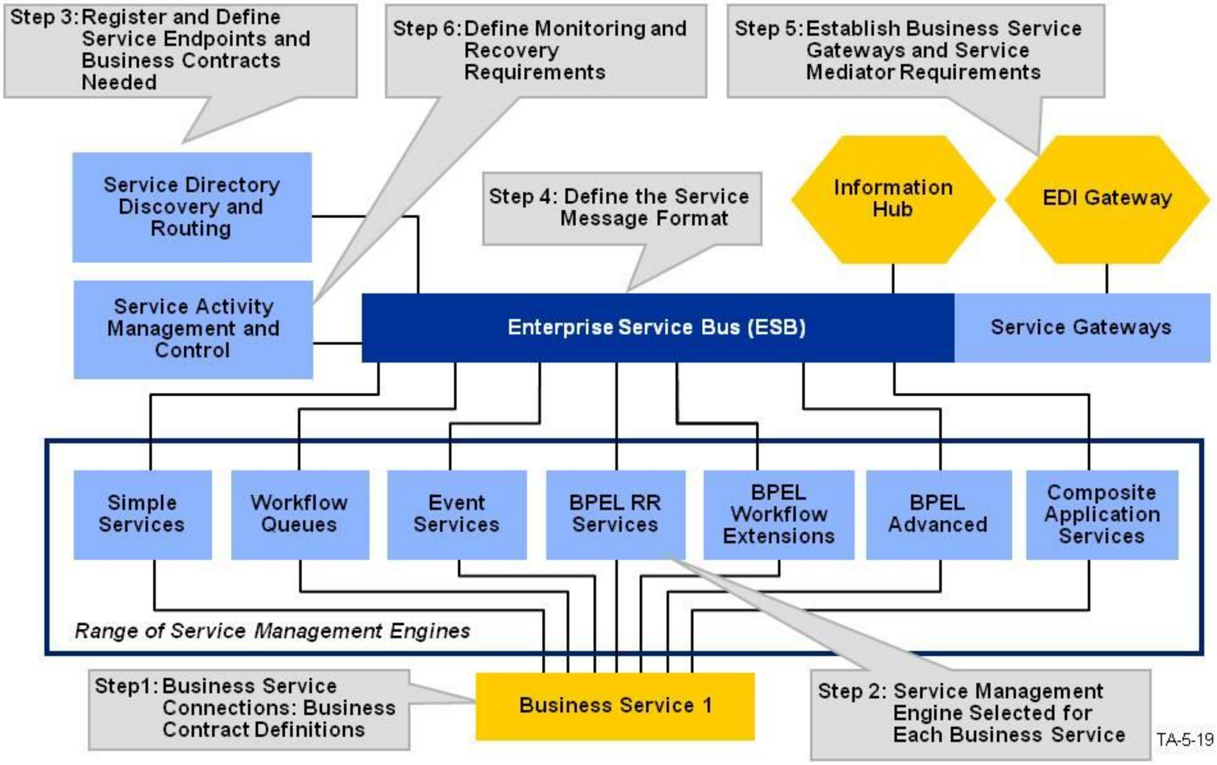
Step 3: Register and Define Service Endpoints and Business Contracts Needed
Step 6: Define Monitoring and Recovery Requirements
Step 5: Establish Business Service Gateways and Service Mediator Requirements
Service Directory Discovery and Routing
Step 4: Define the Service Message Format
Information Hub
EDI Gateway
Service Activity Management and Control
Enterprise Service Bus (ESB)
Service Gateways
Simple Services
Workflow Queues
Event Services
BPEL RR Services
BPEL Workflow Extensions
BPEL Advanced
Composite Application Services
Range of Service Management Engines
Step1: Business Service Connections: Business Contract Definitions
Business Service 1
Step 2: Service Management Engine Selected for Each Business Service
TA-5-19

Figure 5-21. Service Infrastructure – Adding a Business Service

2. **Step 2** – Select the service management engine that meets the service patterns and the behaviors of the SMA.
3. **Step 3** – Define and register the service with a Universal Description, Discovery, and Integration (UDDI) Version 3 compliant registry so that other community registries can link to it. A registry allows the semi-automated discovery and binding of service requests to specific service endpoints and provides information needed to route the service message format to the business and technical service endpoints. The metadata includes a definition of channels, links between business process models (in BPEL) and the messages exchanged, service endpoints, and service contracts as defined in WSDL. CMS will provide more direction and future guidance about registries.

Semi-automation of the Service Directory Discovery and Routing step remains hypothetical and the future of UDDI web service registries is unclear at best. Until the numbers of services becomes critical mass, the process of discovery is a manual process (see Part III, Chapter 2, Technical Management Strategy).

4. **Step 4** – Define the service message format. The ESB uses a generic data format and specific content formats the MITA AA defines and captures in a semi-formal template (the Data Exchange and Sharing Interchange Template) and in a more formal self-

describing XML-based information exchange package. The package includes both WSDL and XML Schema although the execution of the package might not send in the XML format, but in the more compact binary format. These documents and their generated formats allows for easy adaptation and semi-automated testing. Service or business contracts generated tests and extended them with additional tests developed by testers. Test tools for services are critical aspects of service testing and incremental release of services.

5. **Step 5** – The service gateway uses 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.
6. **Step 6** – Monitor cross-services and executive recovery. The MITA AA monitors the performance of service capabilities as it adds them and supports their recovery. Individual service-enabled products have built-in exception reporting, performance standards, and recovery. These features are desirable at MITA Maturity Level 3. CMS expects activity, management, and recovery capabilities at MITA Maturity Level 4. The script that defines the automated and manual steps to recover from failures is an important element of a complete service solution.

Service Invocation and Execution

After the MITA AA has a service added to the infrastructure, the SMA performs five (5) steps to activate the service. These steps are in **Figure 5-22** below.

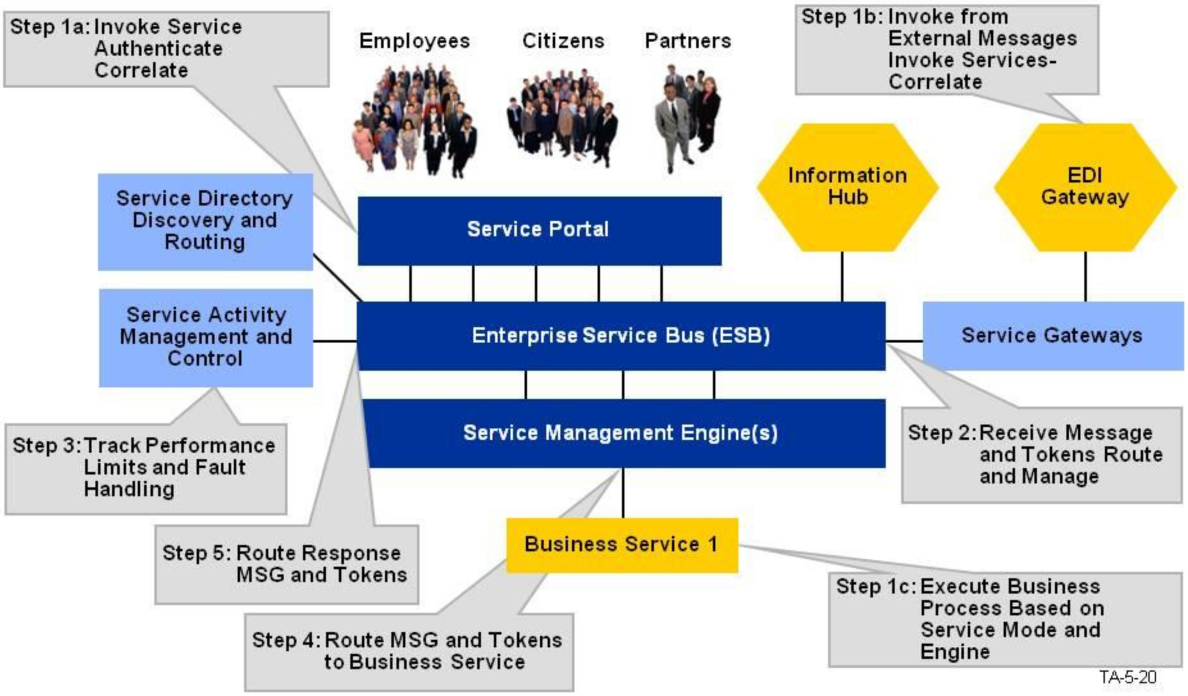

Figure 5-22. Service Infrastructure – Service Invocation and Execution

1. **Step 1: Service Invocation** – The SMA can invoke services in three (3) ways:

   A. **Invoke Service, Authenticate, and Correlate –** Refers to a user at the portal invoking or re-invoking a service 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 will sign on, and the system will authenticate the user's session before starting up the service, at which time the eAuthentication service establishes a token that notes the user's roles and authorizations. The service establishes another token for the types of services the user is 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 –** Initiates a set of services, such as sending in batch messages for all transactions for the day. The series of threads manage batches of services requests which results in a stream of interactions. The ESB and the service portal handle multiple threads of interaction, and the designer configures them based on stakeholder performance needs. External messages come through this path individually or collectively from a trading partner organization or another agency.

   C. **Execute Business Process Based on Service Mode and Engine** – These are the business services themselves that 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.

2. **Step 2**: **Receive Message and Tokens, Route, and Manage –** ESB is a vital component between the different forms of services from the three (3) major sources in Step 1. The service receives the message, relates a token to the service type (correlation set), and attaches an S&P token to the message. It routes and manages the service flow. Some services are more important than other message flow capabilities (e.g., prioritization and alternative path routing depending on performance limits).

3. **Step 3**: **Track Performance Limits and Fault Handling** – Ensures service follows performance policies and agreements addresses fault handling related to recovery and the measures necessary to maintain the quality of service levels.

4. **Step 4**: **Route Message and Tokens to Business Service –** The service management engine routes the message and tokens to the appropriate business service.

5. **Step 5: Route Response Message and Token (Optional)** – If the business service generates a response, it routes to the appropriate service based on predefined orchestration.

Using Application Architecture

The MITA AA is a reference document that identifies the components needed for the infrastructure of the Medicaid Enterprise, and as a requirements document, provides details for a State Medicaid Enterprise infrastructure. The SMA may use the document in this capacity as a source for its Advance Planning Documents (APDs) and requests for solicitations (e.g., Request for Information (RFI), Request for Proposal (RFP)).