

FSA Integration Partner

United States Department of Education

Federal Student Aid



**Data Strategy Enterprise-Wide
Technical Strategies Team
123.1.8 Web Services Strategy**

Task Order #123

Version 1.0

August 29, 2003



Executive Summary

Web services are on the agenda of many CIOs today, but not without raising many questions. Common concerns surrounding Web services include: Are they mature? Are they secure? Will they replace my current infrastructure? These questions must be addressed before making any recommendations. Additionally, there is often confusion between Web services and websites, and therefore when discussing Web services it is of value to start with a common definition.

“Web services” is the name given to application software that uses a collection of standard Internet technologies to make functionality available over a network in a uniform manner. Whereas the World Wide Web makes information accessible to people, Web services target systems. It enables uniform access between systems and leverages the same communication technologies as the Web. Simply stated, Web services allow systems to talk with one another. But this has been possible for years, so what is significant about Web services?

First, Web services allow the Internet to be leveraged, minimizing the need for proprietary communication methods and “hard-wired” connections. Additionally, it standardizes how messages will be formatted and sent between systems. This allows new systems to quickly understand and build interfaces. Finally, Web services through its discovery capabilities can enable access to business services’ “instructions” to better automate implementation procedures. This minimizes, and in some cases eliminates the need for manual communication methods to establish a service between systems.

The vision for Web services at the Federal Student Aid (FSA) organization focuses on enabling access to its services and information, leveraging industry standards to support the use of Web services for exchanges of information, and improving customer self-service by providing additional capabilities through the Web. The goal of this strategy is to identify areas where Web services can best be utilized and review the benefits and business drivers for implementing such a technology at FSA.

The Technical Strategies team collected business objectives, identified gaps and developed options in conjunction with key FSA stakeholders to enable the future vision for Web services. Each of these options was then reviewed and compiled into an overall Web Services Strategy. Below are the prioritized business objectives defined by FSA that relate to Web services. This analysis offers an examination of Web services and the components that support them to help FSA decide whether or not Web services are the right solution to fulfill these objectives:

Rank	Business Objective
1.	Provide access to customer status via centralized means.
2.	Provide access to common calculations as well as lookup and update (corrections) capabilities in a standardized and central location.
3.	Enable Authentication capabilities via Web service.
4.	Enable a pre-population of FSA Web forms using Web services and leveraging information already gathered regarding a customer.

Web Services Business Objectives



Web Services Recommendation

Web services are a maturing technology and current integration trends point to increased levels of internal and external Web services implementations among major Information Technology (IT) organizations. The core set of standards that enable Web services to transport messages between systems have reached the point of industry-wide acceptance making Web services an industry accepted method for information exchange. Additionally, Web services, like all information technology, need the proper security to prevent unauthorized users from gaining access to an organization's information. Although Web services security standards are still evolving, many of the security challenges to securing Web services are being met by common Web security concepts. These concepts can protect access to business capabilities and the data that supports them. Furthermore, Web services can supplement the integrated services platform to uniformly enable business functions and leverage existing investments in infrastructure.

The use of Web services is a viable way for FSA to expand its communication capabilities both internally and externally. It is aligned with the concept of building out business capabilities instead of systems functions. Below are the key Web services recommendations:

- Leverage Web services to allow standard access to system look-up capabilities.
- Integrate Web services technology with the Web Usage Framework to provide access to business capabilities through the Portals.
- Apply Web services security standards to protect access to FSA business capabilities.
- Couple Web services with Business Process Management to enable business capabilities requiring multi-system coordination.
- Enable Web service discovery via a common repository of Web service capabilities.
- Engage a standard governance structure to oversee the implementation for both internal and external Web services.

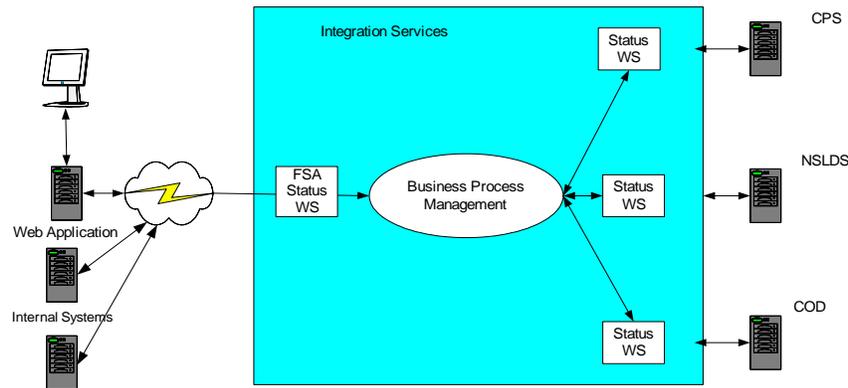
FSA should undertake a phased approach to implement an enterprise solution for Web services. FSA's implementation approach should plan across the enterprise but start off small to successfully realize the benefits that Web services can bring to an integrated solution. First, FSA should look to implement simple business functions internally and then move towards providing access to these capabilities for external trading partners' systems. As simple business capabilities mature and the demand for more integrated capabilities increases, FSA can begin to build composite Web services that leverage data and services from multiple systems.

These recommendations offer a starting point for enabling FSA business services. Below is an example that illustrates these recommendations in practice.

One type of Web service that could be utilized by FSA is a Customer Status Look-up. Because the necessary components to understand the cross-lifecycle status of an FSA customer reside in multiple systems, the Web service for this business capability would be made up of multiple requests targeting different systems. Business Process Management, as discussed in the Internal Data Strategy allows coordination of events between systems. The business process management layer could manage multiple requests to retrieve and compile the data. This



aggregate set of customer status data could then be retrieved in a single FSA status service. Since the end value lies with the users, this result could be posted to the student's portal. Finally, this same functionality could also be made available to a school's system without rewriting any code by making this service available to the external community.



Status Lookup Web Service Example

Web services are not a panacea; they enable open communication when multiple systems require access to the same set of services. To support integration across the enterprise, FSA should create and standardize governance procedures for managing Web services implementation. To avoid duplicative efforts, these procedures should ensure that the enterprise systems collaborate before developing Web services. This governance process could also ensure that standards are employed and Web services are created uniformly across the enterprise. For example, a common set of criteria could be applied to leveraging internal Web services to determine if the new functionality would:

- Satisfy a need for mass accessibility to a common functionality.
- Replace duplicative functionality across multiple systems.
- Be compatible with the existing architecture.
- Support current business processes.
- Enable low volume transactions.

Web services "Discovery" refers to the ability for consumers to locate an enterprise's services and is enabled by advertising their existence through a common means. Discovery and the implementation of discovery standards is another component of Web services that should be addressed by this governance process. FSA needs a discovery mechanism that defines the method of communication between the owner of the Web service and its users. FSA should enable Web service discovery via a common repository of Web service capabilities. Access controls surrounding the discovery repository could secure and monitor access for both internal and external Web services. Some of the benefits of implementing a discovery mechanism include:



-
- Automating access to service definitions to reduce the cost and effort of using the services.
 - Centralized approach to distributing Web service definitions will help ensure that Web services are leveraged consistently by systems and external trading partners.
 - Supports the reuse of Web services by systems internal and external to FSA by publishing the Web services in a centralized location.

The overall benefits that FSA can achieve by implementing the proposed solutions include:

- Enable organizations to more rapidly create and distribute new products and services.
- Increased Operational Efficiency and Quality of Service:
 - Increased accuracy of information gathered by reducing the human error factor.
 - Ability to collect data only once and share the data gathered across departments.
 - Increased efficiency by automating current processes.
- Improved Return on Investment:
 - More efficient use of system resources and extended life of aging technology.
 - Providing consistent flexible access to existing legacy systems.
 - Cost savings by enabling a transaction to be processed without manual intervention.
 - Lowers the overall cost of integration by applying industry wide Internet standards to reduce time to delivery.
- Provides a flexible and agile infrastructure:
 - Improved consistency across organizations.
 - Allows for planned replacement of legacy systems while improving service to constituents.
 - Ability to add new services easily and cost effectively.

Next Steps

This Web Services Strategy will be combined with strategies from the other four technical areas to represent a comprehensive Technical Strategy that is in alignment with the overall FSA Data Strategy effort. The collective picture and the required implementation steps will be outlined in the Technology Vision and Strategic Plan (123.1.12), Data Framework Technical Specification (123.1.4) and Quality Assurance Strategy and Implementation Plan (123.1.5). These documents will serve as the enablers of the high-level Data Strategy business objectives.

In preparation for the delivery of the Technology Vision and Strategic Plan (123.1.12), working sessions will continue to be conducted with key FSA stakeholders through September and October as part of the effort to develop strategies for the remaining technology areas. The Technology Vision and Strategic Plan will be delivered in mid-November.



Amendment History

DATE	SECTION/ PAGE	DESCRIPTION	REQUESTED BY	MADE BY
08/29/03	All	Documented submitted for FSA-wide review.	N/A	K. Michl



Table of Contents

1	INTRODUCTION	9
1.1	PURPOSE	9
1.2	BACKGROUND.....	9
1.3	SCOPE	10
1.4	ASSUMPTIONS	10
1.5	BUSINESS OBJECTIVES AND GAPS.....	10
1.6	KEY DECISIONS POINTS	11
1.7	ASSESSMENT CRITERIA METHODOLOGY	12
1.8	SUBJECT MATTER EXPERT UTILIZATION	13
2	WEB SERVICES BACKGROUND.....	14
2.1	DEFINITION	14
2.2	WEB SERVICES MATURITY	14
2.2.1	<i>Web Services and Business Services.....</i>	<i>16</i>
2.2.2	<i>Government Web Service Implementations</i>	<i>16</i>
3	HOW WILL WEB SERVICES PROMOTE INTEGRATION OF BUSINESS CAPABILITIES?.....	18
3.1	WEB SERVICES BUSINESS PROCESS STANDARDS	22
3.2	OPTION ASSESSMENT.....	23
4	HOW WILL WEB SERVICES BE COMMUNICATED AND MANAGED?.....	26
4.1	WEB SERVICES MARKETING	26
4.2	WEB SERVICE DISCOVERY OPTIONS	26
4.2.1	<i>External Discovery Considerations</i>	<i>28</i>
4.2.2	<i>Internal Discovery Considerations</i>	<i>28</i>
4.2.3	<i>Options Assessment</i>	<i>28</i>
4.3	ENTERPRISE WEB SERVICE GOVERNANCE.....	31
5	HOW WILL WEB SERVICES BE SECURED?.....	32
5.1	WEB SERVICE SECURITY TECHNOLOGIES AND STANDARDS	33
5.2	SECURING WEB SERVICE DISCOVERY.....	35
5.3	COMMUNICATION CHANNEL SECURITY	35
5.4	USER VERIFICATION, AUTHENTICATION AND ACCESS CONTROL	35
5.5	ENTITY VERIFICATION, AUTHENTICATION AND ACCESS CONTROL	36
6	RECOMMENDATION.....	37
6.1	RECOMMENDATION SUMMARY	37
6.1.1	<i>How will Web services promote integration of business capabilities?.....</i>	<i>38</i>
6.1.2	<i>How will Web services be communicated and managed?.....</i>	<i>40</i>
6.1.3	<i>How will Web services be secured?.....</i>	<i>40</i>
6.2	RECOMMENDATION BENEFITS	41
6.3	BRIDGING THE GAPS	42
6.4	ALIGNMENT WITH BUSINESS OBJECTIVES.....	43
	APPENDIX A – BUSINESS OBJECTIVE ACCOMMODATION CRITERIA.....	45
	APPENDIX B – WEB SERVICES STANDARDS	46
	APPENDIX C: MEETING MINUTES – WORKING SESSION #1	51
	APPENDIX D: MEETING MINUTES – WORKING SESSION #2	55



Tables and Figures

Table 1.1 - Web Services Current State Gap Analysis.....	11
Table 3.1 - Web Service Business Process Coordination Business Process Impact Assessment ..	23
Table 3.2 - Web Service Business Process Coordination Flexibility Assessment	23
Table 3.3 - Web Service Business Process Coordination Level of Effort Assessment	24
Table 3.4 - Web Service Business Process Coordination User Impact Assessment	24
Table 3.5 - Web Service Business Process Coordination Assessment Scoring.....	25
Table 4.1 - Web Service Manual Discovery Assessment.....	29
Table 4.2 - Web Service Email Discovery Assessment	29
Table 4.3 - Web Service Secure Web Site Discovery Assessment	30
Table 4.4 - Web Service UDDI Discovery Assessment.....	30
Table 4.5 - Web Service Discovery Options Score Summary	31
Table 6.1 - Recommendation Gap Bridging	43
Table 6.2 - Recommendation Business Objective Fulfillment.....	44
Figure 2.1 - Web Services Framework.....	15
Figure 2.2 - Service-Oriented Architecture.....	16
Figure 2.3 - Australian Tax Office Web Service	17
Figure 3.1 - EFC Calculator Web Service Example.....	19
Figure 3.2 - Borrower Status Lookup Web Service Example	21
Figure 3.3 - Address Update Web Service Example	22
Figure 5.1 - Web Services Security Standards	34
Figure 5.2 - Maturity vs. Features of Security Technologies.....	34
Figure 6.1 - Evolutionary Approach to Web Services.....	39



1 Introduction

1.1 Purpose

The purpose of the Web Services Strategy document is to outline options that may be employed to help FSA reach its Web services vision. This document will expand on the current state and business objectives related to Web services that were captured in the Technical Strategies Statement of Strategic Focus (123.1.6) by clearly documenting options that can be used to fill gaps that exist between the current and target states. This document addresses FSA Performance Plan Action Items 16.5.3 (Develop technical standards and guidelines) and 16.8 (Develop an enterprise Web Services/Portal Strategy) and includes options assessments of solutions that may help FSA align its key technology areas with its overall business objectives. Five strategy documents will be produced for each of the five key Technical Strategies areas in preparation for the delivery of the Technology Vision and Strategic Plan (123.1.12), which will outline the steps to implement FSA's Data Strategy across the enterprise.

1.2 Background

The Department of Education's Federal Student Aid (FSA) organization is seeking to deliver overall improvements in the areas of data quality and data consistency. The goal of implementing improvements to the flow and consistency of data exchange is to ensure that FSA complies with regulations set forth by oversight organizations in support of the program-wide goals, which include maintaining a clean audit and ensuring exclusion from the General Accounting Office (GAO) high-risk list.

The purpose of the FSA Enterprise-Wide Data Strategy is to define FSA's enterprise data vision and strategy for how it will combine the tools, techniques and processes, documented in the FSA Data Strategy Framework, to handle its enterprise data needs. The effort to begin implementing Web services at FSA is one of five technical strategies that when combined with the strategies for Data Framework, XML Framework, Common Identifiers, and Enrollment and Access Management comprise the overall FSA Enterprise-wide Data Strategy. The technical strategies in addition to Web services include Internal Data Exchange, Web Usage (Portals), External Information Access (FSA Gateway), and Data Storage, Management, and Access. Each of these strategies will be addressed in separate documents, but were considered during the development of the overall Web Services Strategy.

In order to create the overall Web Services Strategy for FSA, the current state of Web services at FSA was compiled and validated with key business owners. The current state was then used as a basis for a series of seven business objective gathering sessions from which detailed business objectives with respect to the five technology areas were gathered from FSA business across the student aid lifecycle.

Approximately 200 raw business objectives were gathered for each of the technical strategies key areas. These business objectives were then refined, consolidated, and prioritized by FSA business owners in a series of consensus meetings. The business objectives and associated gaps



between the objectives and the current state of technology at FSA were gathered and presented through the Technical Strategies Statement of Strategic Focus (123.1.6).

The document details how the implementation of additional Web services can help FSA achieve the business objectives that were set forth in the Technical Strategies Statement of Strategic Focus.

1.3 Scope

The goal of this strategy document is to provide options for FSA's vision to improve the use of Web services capabilities between FSA systems and trading partners. The strategies associated with each of the five technical areas will later be combined in the Technology Vision and Strategic Plan (123.1.12) to present an overall technical strategy along with a road map for achievement. The key items that this document will present include:

- An overview of the Web services current state with respect to business objectives.
- Detailed options assessment to outline the future state of enabling Web services technologies.
- Analysis of each technical option, which includes positive and negative impacts as well as gap fulfillment.
- Recommended technical options that will help FSA best achieve the business objectives.

1.4 Assumptions

The following assumptions have been factored into the scope for the Web Services Strategy:

- A three to five year timeframe to implement the technical strategies that will help FSA achieve its business objectives.
- Much of the architecture required to implement Web services at FSA is already in place.
- Since the time of the original business objective gathering sessions, additional projects have been identified as having an impact on the Technical Strategies and FSA's future state. As appropriate, these efforts and other potentially relevant efforts will be assessed for impact during subsequent Technical Strategies deliverables.
- Considerations have been made that account for the future FSA direction of Internal Data Exchange, Web Usage, External Information Access, Web Usage and Data Storage, Management, and Access.
- Real-time data exchange refers to an exchange of data that triggers a series of events across multiple systems as soon as reasonably possible.

1.5 Business Objectives and Gaps

Industry trends indicate that many businesses are moving toward Web service implementations to reduce costs while providing increased levels of customer service. In order to address this trend toward Web services, set of consolidated and prioritized business objectives from the consensus meeting were captured in the Technical Strategies Statement of Strategic Focus (123.1.6). These objectives then served as the primary input for the overall Web services vision.



A group of commonly shared services was identified through these business objective gathering sessions as potential Web services because of the need for consistent relays of information for certain business functions. Some common themes echoed by the business owners included the desire for sets of commonly required services. This strategy focuses its technical option assessment on the ability for the recommended solutions to fulfill the gaps. Based upon the feedback obtained from key FSA business owners, the following table outlines the business objectives and gaps that must be filled to enable desired Web service functionality. Explanations of the assessment criteria can be found in Appendix A: Business Objective Accommodation Criteria.

Rank	Business Objective	Percent Realized	Gaps
1.	Provide access to customer status via centralized means.		<ul style="list-style-type: none"> No means to enable common access to customer status. No externally communicated Web services.
2.	Provide access to common calculations as well as lookup and update (corrections) capabilities in a standardized and central location.		<ul style="list-style-type: none"> No common calculations enabled via Web service Some look-up and update capabilities exist but none are standard, centralized or using Web services.
3.	Enable Authentication capabilities via Web service.		<ul style="list-style-type: none"> PIN authentication Web Service is in place, but not utilized. Security model is not in place to support service. A diverse set of authentication functionality being utilized.
4.	Enable a pre-population of FSA Web forms using Web services and leveraging information already gathered regarding a customer.		<ul style="list-style-type: none"> Limited pre-population functionality exists for the FAFSA (Free Application for Federal Student Aid) but does not leverage any Web services.

Table 1.1 - Web Services Current State Gap Analysis

1.6 Key Decisions Points

Based upon the business objectives and gaps that were identified in the previous section, a series of key decision points were established and refined by key cross-lifecycle business owners. The purpose of these decision points is to provide guidance in developing options and an ultimate solution recommendation.

- **What are the key Web services that FSA should enable?**

Currently, no Web services are being utilized at FSA for either internal or external information exchange. As FSA looks to improve both customer service and interaction with trading partners, business processes should be analyzed to determine if services can be consolidated and reused. Identifying which services can be deployed for use by systems both inside and outside the enterprise is a necessary exercise to address this



question.

- **How will Web services be used internally and externally?**

Web services can be used both internally and externally to consolidate common logic for use by multiple systems. The approach to creating, publishing, and accessing Web services needs to be analyzed with respect to both internal and external systems.

- **What standards will be employed to enable Web services?**

Many standards exist with regards to the development, deployment, and publishing of enterprise-level Web services. A review of these standards is required to provide a consistent approach to utilizing Web services.

- **How will Web services information be communicated to external partners?**

In addition to the common set of standards applied to Web service deployment, additional consideration should be made when exposing FSA Web services to the external community.

1.7 Assessment Criteria Methodology

In an effort to assess each option effectively, the business owners established a set of assessment criteria. These criteria should be used with the business objectives and key decision points in order to determine each option's true value to FSA.

This set of rating criteria was applied to enable the consistent comparison of options to one another so that it is readily apparent as to which option best serves FSA's future needs. The results of this comparison serve as the basis for determining what the overall technical strategy recommendation is going forward.

The following assessment criteria were used to evaluate each option:

Business Process Impact – Does the option have the potential of introducing significant cross-lifecycle business process improvements?

Flexibility – Does the option offer improved flexibility for Web services? Can the option support both existing legacy systems and potential future systems?

Level of Effort – Will significant effort (time and resources) be required to realize this option? Will the amount of effort required to maintain FSA Web services be reduced?

User Impact – Will the end user experience improvements with this option?



1.8 Subject Matter Expert Utilization

The following Subject Matter Experts (SMEs) were leveraged during the creation of the Web Services Strategy:

1. Anthony Roby, Accenture Web Services Global Lead
2. Dorival Simoes, Accenture Web Services Program Manager



2 Web Services Background

The following sections are intended to provide background information on Web services. Questions such as “What is a Web service?” and “What is not a Web service?” will be addressed. In addition, the maturity of Web services will be explored and some examples of government Web services implementations presented.

2.1 Definition

Managing the information needs of internal users, citizens and trading partners is a growing imperative for government agencies. One of the challenges facing government agencies such as FSA includes breaking down the silos of information that currently exist between internal organizations and other government agencies to promote increased amounts of information sharing and the streamlining of business processes. These challenges are coupled with citizens’ demands for easier access to data.

“Web services” is the name given to application software that uses standard Internet technologies to make functionality available over a network in a uniform manner. This standardization is one of the key benefits to using Web services. Web service use helps to ensure that service description, message formatting, message encapsulation, and service discovery are uniform across all systems and platforms.

Web services can be used to enable a variety of business functions. Initial internal implementations often focus on simple data lookups that enable real-time standardized access to system information. For example, FSA could create a Web service that is capable of retrieving a particular customer’s status from a system.

Web services should not be confused with other methods of data exchange that make use of Internet technologies for communication. For instance, some Web pages may utilize Web services to provide some functionality, but Web pages should not be considered Web services themselves. Additionally, system-to-system connectivity that is achieved through either proprietary means or “hard-wired” methods are not considered Web services, as they do not use the same levels of standardization.

2.2 Web Services Maturity

While many IT organizations see Web services as an evolving technology, current integration trends point to increased levels of internal and external Web services implementations among major IT organizations. A recent Dataquest survey was commissioned by Gartner in February 2003 to provide insight into the trends surrounding Web services over the next 12 to 24 months.

A key finding of this survey was that, “Fifty-four percent of respondents noted they used/plan to use (over the next 12 months) Web services to integrate applications both within the organization (interenterprise) as well as with partners or customers (intraenterprise). During this same time frame, 39 percent used/plan to use Web services only within their organization. When asked what the scope of the organization's strategy was over the next 24 months,



respondents using/planning to use Web services both intra- and interenterprise jumped to 65 percent, whereas respondents limiting Web services projects to only within the enterprise dropped to 23 percent.¹

From the results of this survey, one could conclude that Web services are becoming an accepted if not preferred means of exchanging data both inside and outside of the enterprise. It is also apparent that Web services usage for enterprise-to-enterprise data exchange is also increasing.

While the use of Web services becomes more commonplace, some of the standards associated with Web services continue to evolve. The core set of standards that address message format, encapsulation, transport, description, and discovery have reached the point of industry-wide acceptance. The standards that dictate more advanced Web services functions such as business process management, transaction services, and security, are still evolving. The following diagram illustrates the Web services standards as they apply to different functions – the red boxes indicate categories where standards are less mature. Some of these standards are addressed in detail in Appendix B – Web Services Standards.

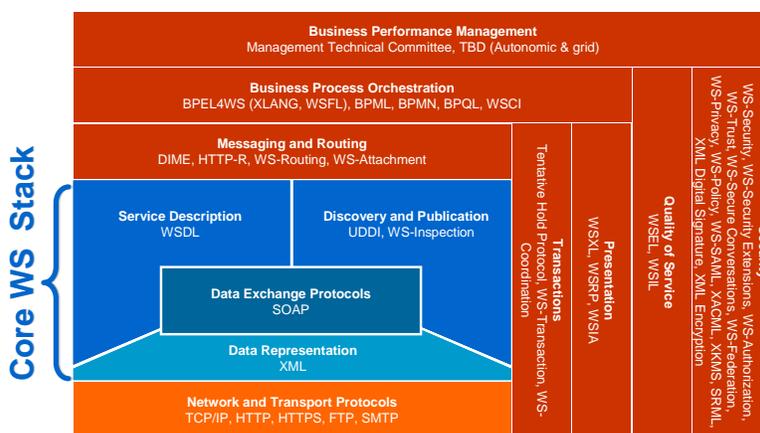


Figure 2.1 - Web Services Framework²

While the major standards entities, the Organization for the Advancement of Structured Information Standards (OASIS) and the World Wide Web Consortium (W3C), continue to develop some advanced standards, the active evolution of standards should not be seen as a limitation for implementing enterprise Web services. This evolution implies the necessity to reevaluate some standards as major shifts in technology direction occur.

¹ © Gartner, Inc. Source: “2002-2003 Web Services Development, North America (Executive Summary), 3 July 2003.

² © Accenture Web Services Point of View, March 2003.



2.2.1 Web Services and Business Services

A Web service is typically thought of as enabling a single business capability for use by many people or systems. For example, MapQuest utilizes Web services to enable outside entities such as travel agencies, retail stores, and hotels to provide driving directions easily to their customers. Additionally, groups of Web services can act in concert to provide end-to-end business process solutions as part of a service-oriented architecture. The following diagram illustrates how multiple Web services can interact to enable a service-oriented architecture:



Figure 2.2 - Service-Oriented Architecture

The key purpose of a service-oriented architecture is to create and expose multi-function business capabilities via Web services rather than through application or system-based functions. This is different from traditional forms of application design in that business functionality is enabled through groups of distinct services that are provided directly to customers. While the terms “Web services” and “service-oriented architecture” are closely related, they should not be used interchangeably. FSA needs to not only consider simple functions that they might want to enable but also the business capabilities as they relate to the student aid lifecycle.

2.2.2 Government Web Service Implementations

Government agencies must be able to provide reliable 24/7 access to citizens and trading partners. For any new systems that are implemented by government agencies, special consideration must be given to the maturity and reliability of the proposed technology as well as to the related implementation risks. These considerations are no different for FSA with respect to Web services, but they must be balanced with the end value that Web services can provide to FSA’s ultimate customers. The United States Air Force and the Australian Tax Office are examples of government agencies that have successfully realized this balance with Web services implementations.

The United States Air Force (USAF) is developing Web services to provide command and control functions for its Theater Battle Management Core System (TBMCS). Once developed, USAF will use Web services to assist in the planning and execution of future wars. The USAF has recognized that Web services can provide immediate value to its agency because they enable a more efficient, less costly, and faster interface for maintaining the TBMCS. In addition, Web services can provide a means for the USAF to quickly integrate new capabilities into its systems with minimal impact to established components.

In addition to the USAF, the Australian Tax Office (ATO) recently created a business portal enabled with Web services to allow government agencies, businesses, and citizens to interact



with one another. The portal provides a user interface to a Web service that is capable of performing a search based upon the unique business identifier. It also provided the capability to update business information online. The following diagram illustrates how Australian citizens can interact with government agencies through a single portal with business functions enabled via multiple Web services:

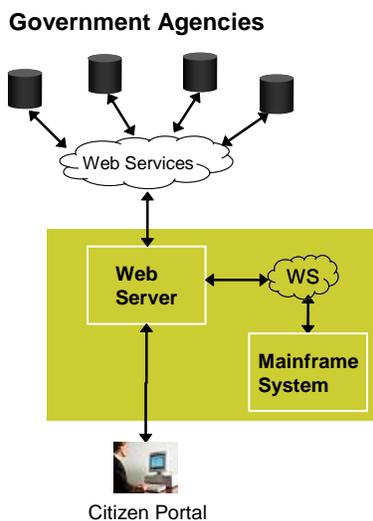


Figure 2.3 - Australian Tax Office Web Service

The ATO realized significant business value using Web services in that the technologies involved enabled business to immediately obtain their unique business identifier. Additionally, the amount of customer support required by customers conducting business with the ATO decreased dramatically as most transactions now require no support from ATO operators. Finally, Web services have promoted increased levels of information sharing between different Australian government agencies.



3 How will Web services promote integration of business capabilities?

Today FSA's business functions are managed by multiple independent systems that are typically aligned with one phase of the student aid lifecycle. This creates a very system specific implementation which requires knowledge of each system and the services they provide. Ideally both internal and external users should not have to understand the systems or their role in providing services, but rather they only need to understand the business processes that enable the aid lifecycle. Web services are powerful tools that enable evolution from this system oriented structure to more business process-based integration that helps to minimize the user's necessity to understand system specific information.

The current environment creates challenges for integrating business functions. Today minimal capabilities exist to enable real-time data exchange between different FSA systems. In addition, minimal business process coordination takes place between systems that serve different phases of the student aid lifecycle. This lack of information sharing coupled with minimal business process coordination results in no automated means to easily determine the status of a given borrower at a given stage in the lifecycle.

In addition, the siloed nature of FSA systems also prevents reuse of common functionality across the enterprise and contributes to data quality issues. For example, calculation logic that is owned by a particular system often has to be duplicated by other systems or trading partners because there is no effective method to share business capabilities. In terms of data quality, updates to data that are performed on one system are often not effectively communicated and performed on other systems. This results in inconsistencies across various phases of the lifecycle.

There may be opportunities to consider Web services as a means to improve integration, as well as further the evolution towards business process based-services. This is enabled by the fact that Web services can complement the existing integration platform rather than replace it. Web services further promote integration by:

- Enabling access to common business functions needed by the internal and external community.
- Providing business services to the Web.
- Providing real-time access to existing legacy systems.

Enabling Common Business Functions

There is an ever-increasing need for real-time data exchange within the FSA enterprise and with FSA trading partners. This real-time exchange, however, does not necessarily require Web services. The existing Enterprise Application Integration (EAI) infrastructure can be leveraged to provide real-time communication between systems. For example, today the real-time communication between FAFSA on the Web and CPS (Central Processing System) is handled by the existing integration platform.



In situations where a business function could be consumed by multiple systems, Web services should be considered over proprietary integration methods. An example of such a business function is the Estimated Family Contribution (EFC) calculation that is currently implemented by CPS.

The EFC calculation is currently owned and implemented by CPS, but the ability to perform the EFC calculation is desired by other FSA systems and trading partners in the external community (schools). In order for other systems to make use of this functionality, the logic required to perform the EFC calculation must often be duplicated by each system that needs to perform the EFC calculation. For example, Sallie Mae currently implements its own version of the EFC calculator to give potential borrowers an idea of how much their EFC might be. Additionally, the Common Origination and Disbursement (COD) system also implements a version of the EFC. Making this type of functionality commonly available can minimize the discrepancies between systems by enabling a single source for the information and business capability.

A Web service could be implemented to facilitate access to this type of common service. Web services could make the CPS EFC calculation centrally accessible to all internal systems, FSA portals, as well as to trading partners with appropriate credentials that reside outside of the enterprise. By enabling the EFC in a centrally accessible manner, the discrepancies and confusion that are associated with the calculation methods currently used by trading partners can be reduced if not eliminated. The following figure illustrates an example of a centrally accessible EFC calculator:

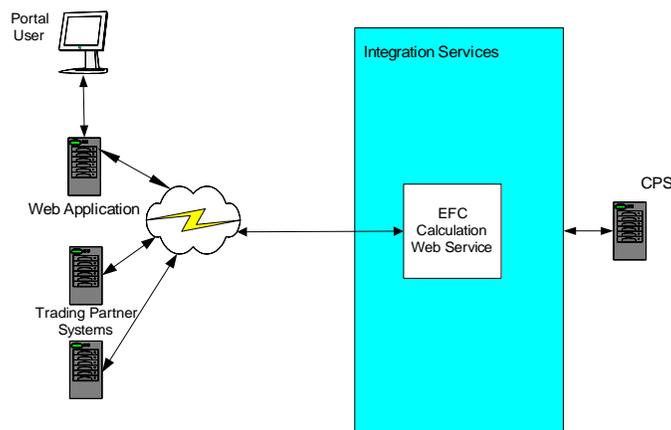


Figure 3.1 - EFC Calculator Web Service Example

In order to determine what common business functionality should be enabled as a Web service, a key set of criteria should be established for enterprise Web service usage. This set of criteria would ensure that Web services are consistently applied and leveraged across the enterprise.



Providing Business Services to the Web

A Web service can enable simple, real-time access to a system. To provide this capability, a Web service could be enabled on a system that upon receipt of identifier information provides a return message containing status information. This would allow the caller of the Web service to obtain status information on a student from a single system. This service could then be coupled with the portal or Web infrastructure to make this capability available to external users via the Internet.

The benefit over directly connecting to a system or the system's database is that any third party website that has permissions to access this service can now provide student status. In addition, the system that invokes the Web service would be shielded from any changes that are made to the source system's data storage or processing logic.

Although this simple status Web service makes a single function accessible in a standard way to many sites or systems, it does not provide FSA with significant value by itself. In most cases, the user is most interested in the status across multiple systems. Multiple Web services (composite Web services) can help bridge this gap by working in concert with other components of the integration platform.

The business process management layer is responsible for the definition and management of business processes that span multiple applications across the enterprise. This enables the communication of not just data, but also the business process context of the data being sent to other applications. It is from the aggregation of integration services that the greatest business value can be achieved. Therefore, coupling Web services with business process management capabilities, while potentially leveraging existing EAI capabilities can provide users with information from disparate systems.

Determining a particular borrower's status in the financial aid lifecycle currently requires inquiries of multiple systems and manual analysis of customer data. Composite Web services could be used to enable an improved ability to determine customer status through the use of business process management capabilities to coordinate status requests across multiple back-end systems. The business process management layer could also handle scenarios such as conflicting status, missing status, or simply perform aggregation of information. The result would be an integrated status that can be accessed in a standard way by systems with appropriate credentials.

This type of customer status service could be utilized internally by the portals or even externally by school sites. The following diagram illustrates the concept of a composite Web service that is capable of providing customer status data:

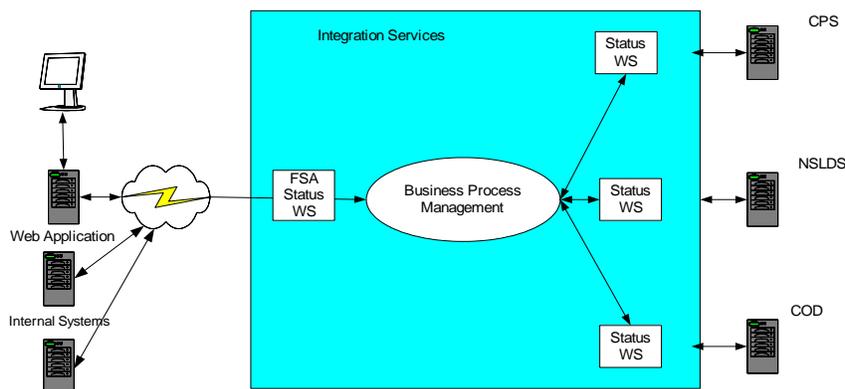


Figure 3.2 - Borrower Status Lookup Web Service Example

Some of the benefits of combining multiple integration services include:

- Centralized visibility and control of multi-step business processes traversing multiple applications and enterprises.
- Real-time analysis capabilities across and between enterprises.
- Transactional control across the applications and between enterprises.
- Process state maintained across multiple systems.

Providing Real-time Access to Legacy Systems

Gaining access to legacy system information in a real-time fashion is often a challenge. Access across the enterprise (or outside if appropriate) to business functions is typically self-contained and accessible only by proprietary communication mechanisms. Web services can provide systems open access to these types of services. For example, as part of the Standard Student Identification Method (SSIM), when modifications are made to a borrower's data on a single source system, updates to the data across multiple systems could be provided via Web services. As address information is updated in one system, Web services could be leveraged to update the other systems in the financial aid lifecycle (as appropriate), based on a set of business rules.

To enable that functionality, a set of centrally accessible "address updates" Web services could be developed and exposed on each source system requiring the service. As updates are necessary, these services could be invoked as appropriate to provide data distribution to multiple systems. By making these updates Web service-based, the same service could be provided to a website to allow students to perform address updates as well. By using Web services, it is possible for all websites, systems and users to leverage the same capability to perform a common business process. The business rules that define the address update process order could be executed by the business process management layer of the integrated services platform. This address update example is illustrated below:

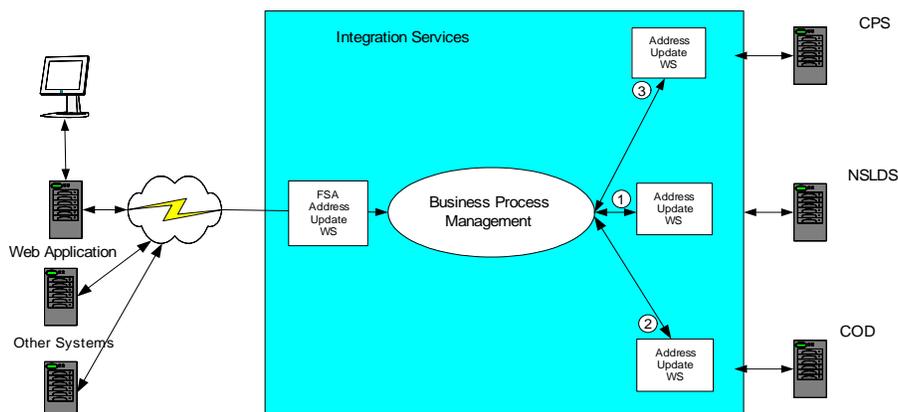


Figure 3.3 - Address Update Web Service Example

As mentioned in the earlier borrower status example, Web service coordination, the integration platform and business process management services would allow the address update method to be more intelligent. The routing, decisions, and execution of address updates across the system could be modeled in the business process engine and executed via a mix of Web services and existing communication methods. The business needs of the solution would drive the complexity and the effort required to implement the integration solution.

Some benefits of providing real-time access to legacy systems include:

- Extending the lifespan of legacy applications by enabling their inclusion in more modern architectures.
- Providing centralized access to legacy business logic.
- Increasing the overall transactional capabilities of the architecture.

3.1 Web Services Business Process Standards

Standards are developed to make existing processes easier. There are many business process management toolsets on the market today. However, there is a push to leverage a common language for business process management, an integration component that is extremely valuable when integrating complex services-based solutions. As most technologies and standards surrounding Web services are seen by industry leaders as relatively mature, standards with respect to Web service business process management are continuing to evolve. At present, the emerging Web service standard with respect to business process management is the Business Process Execution Language (BPEL).

BPEL has been developed by BEA, Microsoft, Siebel, SAP, and IBM in conjunction with the OASIS standards consortium and is a result of the convergence of the earlier IBM XLANG and Microsoft's Web Service Workflow Language (WSFL). According to OASIS, BPEL provides the following with respect to Web services³:

³ Business Process Execution Language for Web Services Version 1.1, OASIS, 5 May 2003.



- A model and language for describing the behavior of a business process.
- Processes defining how multiple service interactions are coordinated to achieve a business goal, as well as state and logic that is necessary for the coordination.
- Systematic mechanisms for dealing with business exceptions and processing faults.
- Mechanism that defines how individual or composite services within a process are compensated in the case of exceptions or rollback requests.

As the various standards organizations continue to solidify the business process standards for Web services, it will be necessary to reevaluate the standards for Web service business process coordination as shifts in technology direction occur.

3.2 Option Assessment

The following tables present assessments of how Web services business process coordination will impact existing business processes, flexibility, level of effort, and users at FSA:

Business Process Impact	Does the option have the potential of introducing significant cross-lifecycle business process improvements?	 1.....2.....3.....4.....5 Negative Business Process Impact Positive Business Process Impact
Points	Comments	
 Improved collaboration capabilities.	<ul style="list-style-type: none"> • Business process logic can enable process coordination across multiple lifecycle phases. • Web services allow for increased amounts of data sharing between systems. 	
 Enterprise-wide business process changes may be required.	<ul style="list-style-type: none"> • Current business processes would require modification to take advantage of information and service sharing capabilities. • Increased levels of coordination must occur between different system owners. 	

Table 3.1 - Web Service Business Process Coordination Business Process Impact Assessment

Flexibility	Does the option offer improved flexibility for Web services? Can the option support both existing legacy systems and potential future systems?	 1.....2.....3.....4.....5 Not Flexible Highly Flexible
Points	Comments	
 Increased enterprise flexibility.	<ul style="list-style-type: none"> • Services can be enabled and accessed by different systems as needed. • Web services allow for easy distribution of data and capabilities to external partners. 	
 Web services allow for a phased deployment approach.	<ul style="list-style-type: none"> • Groups of like services can be implemented when business dictates. • Systems can be enabled for Web services in ways to minimize impacts to FSA's business. 	

Table 3.2 - Web Service Business Process Coordination Flexibility Assessment



**Data Strategy Enterprise-Wide
Technical Strategies
Web Services Strategy**

Level of Effort	Will significant effort (time and resources) be required to realize this option? Will the amount of effort required to maintain FSA Web services be reduced?	 1.....2.....3.....4.....5 Significant Effort Required Minimal Effort Required
Points	Comments	
👍	Reduced maintenance effort in the long term.	<ul style="list-style-type: none"> Centrally maintained functionality results in reduced maintenance costs. Modifications to individual systems have less impact to other systems within the enterprise as Web services provide decoupling of functionality.
👍	Reduced development effort.	<ul style="list-style-type: none"> Web services definitions allow internal and external developers to more easily develop applications that make use of FSA services.
👎	Significant effort may be required to implement Web services across the enterprise.	<ul style="list-style-type: none"> Web services are not currently being utilized at FSA. Many systems may have to be Web service enabled.

Table 3.3 - Web Service Business Process Coordination Level of Effort Assessment

User Impact	Will the end user experience improvements with this option?	 1.....2.....3.....4.....5 Negative Impact to User Positive Impact to User
Points	Comments	
👍	Increased levels of customer service.	<ul style="list-style-type: none"> Increased amounts of data sharing and process coordination across the enterprise lead to increased levels of customer service. Web services can better enable self-service capabilities in FSA's portals.
👍	Reduced effort by internal FSA users.	<ul style="list-style-type: none"> Data sharing and process coordination across the enterprise will reduce data inconsistencies and manual reconciliation that occurs between systems. Business process management will better enable troubleshooting capabilities across the enterprise.

Table 3.4 - Web Service Business Process Coordination User Impact Assessment



Score Summary

Business Process Impact	Flexibility	Level of Effort	User Impact
4	5	4	5

Table 3.5 - Web Service Business Process Coordination Assessment Scoring



4 How will Web services be communicated and managed?

To ensure success for an enterprise-level Web service implementation, uniform approaches to communicating and managing Web services capabilities should be taken. Organizations communicate and publish their Web services through a set of “discovery” methods. Discovery is an industry term used to define the mechanisms by which an organization can look-up Web services definitions and understand how to invoke a service. A detailed approach to Web service discovery is needed to ensure that the availability and capabilities of FSA Web services are communicated effectively to both FSA trading partners and the internal community.

The implementation of Web services should leverage a set of centrally managed processes and actions to control the use of this technology. A consistent approach to Web services governance is required to ensure that they are implemented in a uniform manner across the enterprise and that functionality is not unnecessarily duplicated by different services. Additionally, Web services governance provides a means to enable discovery, coordinate integrated services across the enterprise and enforce the use of the proper standards.

4.1 *Web Services Marketing*

One of the first questions with respect to Web service discovery that must be answered is how will FSA system owners as well as external trading partners know that FSA Web services exist? A marketing approach that is focused on communicating the existence of enterprise Web services is key to ensuring that the benefits of Web services are realized by users both within and outside of the enterprise. Communication of Web service availability could take place via the Frequently Asked Questions (FAQ) pages on the FSA portals, via email notification, or even via written memo. The key message is that without effective communication of the existence of Web services it is likely that they will never be used.

4.2 *Web Service Discovery Options*

Once the availability of Web services has been communicated across the enterprise and to external partners, the next step is to enable discovery of Web services so that entities can effectively leverage services within their own systems. Several approaches to Web service discovery may be taken ranging from manual to fully automated means. The following subsections address each of the possibilities for Web service discovery that FSA could employ.

Manual Means

One method for providing Web service discovery is to use manual means to distribute details associated with available services. Using this method, information about Web services would be communicated by methods such as the telephone or printed memos. Users who needed access to a particular FSA Web service would contact the owner of the service and obtain the necessary information required in order to access and invoke the service. If changes to a service implementation occur, FSA would have to manually communicate changes to the user community.



Email

Building upon manual methods of Web service discovery, Email could also be used to communicate Web service implementation details to the user community. FSA could maintain mailing lists, which would be used to distribute service details and changes to interested parties. Users would still need to contact FSA directly in order to receive service access and details.

Email would also enable the capability of electronically distributing Web Service Description Language (WSDL) files that contain Web service descriptions in a format that can be interpreted by application development tools. As with manual discovery, any changes to a Web service description would require targeted communications to service users.

Secure Website

Another more automated means of enabling Web service discovery would be to post WSDL files for given services to a secure website which has access controls and other security measures in place. Once system developers are given access to the secure website, the WSDL for a given Web service can be downloaded and utilized to enable access to FSA systems.

While the secure website would provide capabilities to easily access and download Web service descriptions, FSA would still need to coordinate the communication of service availability as well as service changes to the service users. This communication could be achieved by Email or manual means.

Universal Discovery, Description, and Integration (UDDI)

FSA could also leverage fully automated means of Web service discovery through the use of a UDDI repository. The UDDI protocol is the industry accepted standard for publishing Web services developed by the OASIS consortium. A UDDI repository enables individuals, companies, and applications to dynamically locate and use Web services over the Internet. An enterprise-level UDDI repository would provide the following services:

- A mechanism for FSA to advertise the existence of their Web services and for Web service users to locate Web services of interest.
- Data, metadata, bindings, pointers, and documents for finding and invoking Web services.
- Client and server APIs for publishing to, editing, and querying UDDI repository entries.
- Enable both FSA and trading partner developers to more easily integrate Web service calls into their Web applications.

An enterprise can achieve a greater return on investment when a UDDI is utilized to centrally store several Web services. As the number of Web services produced by an enterprise grows, a UDDI can help with managing the discovery and publication of its Web services.



4.2.1 External Discovery Considerations

When enabling access and discovery of Web services to trading partners outside of the FSA environment, special considerations must be made to ensure that maximum levels of security are met while the availability of services is communicated effectively to the external community.

- External FSA Web service capabilities should be provided in a location that is centrally accessible to trading partners to ensure that the availability of services is effectively communicated.
- The means of discovering Web services should only be given to trusted trading partners to help ensure that members of the public do not know about the FSA Web service capabilities that are externally available.
- To control access to discovery methods, authentication should be required where possible. Requiring authentication will help to ensure that only authorized FSA trading partners have access to the FSA service discovery capabilities.
- Access should further be restricted to ensure that trading partners only have access to services that are applicable to their specific role. For example, a guarantor should not be given access to Web services that are specific to the financial aid application process.

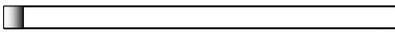
4.2.2 Internal Discovery Considerations

Like externally facing Web services, special considerations must also be made with respect to enabling Web services discovery for Web services that are only intended for use by FSA internal systems. While the security requirements associated with the discovery of internally facing Web services are not as stringent as those for external Web services, the following areas should be considered:

- Internal FSA Web service capabilities should be provided in a location that is centrally accessible to FSA system and business owners to ensure that the availability of services is effectively communicated.
- Service discovery capabilities should be restricted based upon user roles to ensure that internal FSA users and systems can only discover services that are applicable to their respective roles.

4.2.3 Options Assessment

The following tables present assessments of each Web service discovery method presented above:

Manual Means	Web service discovery is enabled via manual means such as telephone, memo, etc.	 1.....2.....3.....4.....5 Less Favorable More Favorable
Points	Comments	
 No new technology implementations required.	<ul style="list-style-type: none"> • Existing methods for communication are used to convey service availability and details. • May enable early means of to Web services usage. 	



**Data Strategy Enterprise-Wide
Technical Strategies
Web Services Strategy**

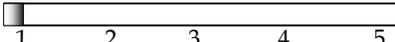
Manual Means	Web service discovery is enabled via manual means such as telephone, memo, etc.	 1.....2.....3.....4.....5 Less Favorable More Favorable
	Inefficient means of distributing new service descriptions to users.	<ul style="list-style-type: none"> Manual processes are not well suited for mass distributions of information. Non-electronic means of distributing service descriptions will lead to increased human error when implementing services.
	Inefficient means of communicating service changes.	<ul style="list-style-type: none"> When changes occur to services, a significant amount of time may be required for notification and compliance of users. No guaranteed way of knowing if all users are properly notified of changes.
	Increased levels of customer support required.	<ul style="list-style-type: none"> Non-electronic means of distribution will lead to increased support requests. Developers will have no electronic basis for development as service descriptions are not provided.
	Manual distribution of service descriptions is not secure.	<ul style="list-style-type: none"> Communications could be intercepted and used maliciously.

Table 4.1 – Web Service Manual Discovery Assessment

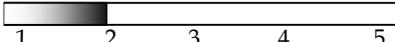
Email	Web service discovery is enabled via Email communication.	 1.....2.....3.....4.....5 Less Favorable More Favorable
Points	Comments	
	Existing technologies can be used to enable discovery of services.	<ul style="list-style-type: none"> Email is a well-established means of communications. May provide initial ability to communicate Web service descriptions.
	Electronic means of service discovery communication and description.	<ul style="list-style-type: none"> Electronic distribution adds some level of delivery assurance. Ability to distribute WSDL to end users in an electronic format will speed development efforts for users.
	Ineffective means of communicating availability of new services and changes to existing services.	<ul style="list-style-type: none"> Email may go unread resulting in critical service changes being missed. Email delivery may be delayed due to network or server issues.
	Requires considerable effort on FSA’s part.	<ul style="list-style-type: none"> FSA must actively manage email distribution lists to ensure communications regarding services go to the correct individuals. New services and changes to existing services must be proactively communicated to affected users.
	Email distribution of services is not secure.	<ul style="list-style-type: none"> Email is not a secure method of communication. Email between FSA and trading partners travels over the public Internet and, without encryption could be intercepted by an individual with malicious intent.

Table 4.2 – Web Service Email Discovery Assessment



**Data Strategy Enterprise-Wide
Technical Strategies
Web Services Strategy**

Secure Web Site	Web service discovery is enabled via WSDL publication on a secure website.	 1.....2.....3.....4.....5 Less Favorable More Favorable
Points	Comments	
👍	Existing technologies used to enable Web service discovery.	<ul style="list-style-type: none"> Technology required to implement a secure website is readily available at FSA. Provides a centralized location for Web service discovery. Promotes reuse of enterprise-level services.
👍	Electronic means of service discovery communication and description.	<ul style="list-style-type: none"> Secure websites provide increased levels of guaranteed delivery for service descriptions. Ability to distribute WSDL to end users in an electronic format will speed development efforts for users.
👍	Secure website provides increased levels of security for discovery.	<ul style="list-style-type: none"> Authentication can be required for access to the secure website. Access controls can be in place to limit discovery of Web services to particular user groups. SSL (Secure Sockets Layer) provides secure communication of WSDL to users.
👎	No effective means to easily communicate new services or changes to existing services.	<ul style="list-style-type: none"> FSA must still address how and when communications regarding new services and changes to existing services occur. Communication of changes to services may not reach affected users in a timely manner.

Table 4.3 – Web Service Secure Web Site Discovery Assessment

UDDI Repository	Web service discovery automated UDDI repository.	 1.....2.....3.....4.....5 Less Favorable More Favorable
Points	Comments	
👍	Fully automated electronic means of Web service discovery.	<ul style="list-style-type: none"> Web services discovery is fully automated. Provides a centralized location for Web service discovery. Promotes reuse of enterprise-level services.
👍	Reduced levels of FSA interaction required.	<ul style="list-style-type: none"> UDDI repository reduces the need for FSA to actively communicate service changes directly to users. Automated WSDL distribution reduces confusion when implementing FSA services. Reduced FSA interaction will result in decreased support costs.
👍	UDDI repository can enable secure discovery of Web services.	<ul style="list-style-type: none"> Authentication can be required for access to the UDDI repository. Access controls can be in place to limit discovery of Web services to particular user groups. SSL provides secure communication of WSDL to users.

Table 4.4 – Web Service UDDI Discovery Assessment



Score Summary

Manual Means	Email	Secure Web Site	UDDI Repository
1	2	4	5

Table 4.5 - Web Service Discovery Options Score Summary

4.3 Enterprise Web Service Governance

In addition to enabling Web service discovery capabilities, FSA should consider how best to govern Web services implementations across the enterprise. A consistent approach to Web service governance can help to ensure the successful deployment of Web services both within and outside of the FSA enterprise. Some the following are examples of considerations that FSA may want to make if developing an enterprise approach to Web service governance:

- Centralized storage and access to enterprise-level Web services.
- Versioning of Web service definitions and XML schemas.
- Standards for development and deployment of Web services both internal and external to FSA.
- Standards for efficiently notifying both internal users and external trading partners of Web service availability.
- Standards for how FSA Web services should be defined using WSDL.
- Consistent application of user and system roles along with defined access levels.
- A detailed approval process for users and systems to control access to Web service discovery, access, and usage capabilities.



5 How will Web services be secured?

Based upon industry surveys, security is one of the main areas of concern for organizations that are currently implementing Web services. This is particularly true for government agencies as the privacy of citizens must be protected and the integrity of government services upheld as business is conducted over the public Internet. The *Privacy Act*, *Government Information Security Reform Act*, and the *Federal Information Security Management Act* are examples of legislation that address information security in government.

While trust is an important component of security for any traditional form of data processing, it becomes even more requisite when dealing with Web services. Increased levels of trust foster better business relationships with clients, customers, and trading partners. To ensure the maximum levels of trust, the following issues must be addressed:

- Communication takes place via the public Internet rather than secure Virtual Area Network (VAN) and Private Managed Network communication channels. How do we guarantee that no one is eavesdropping on or tampering with a business application action as it is performed over public networks?
- Web services involve servers interacting directly with one another. How do we verify that requesting and/or processing systems are not imposters?
- Since Web services are often used for enterprise-to-enterprise data exchange, participating parties must establish and adhere to policies and procedures for trusted Web services.
- As Web services enable the distribution of business logic and transactions across multiple systems and enterprises, how do we ensure transaction integrity when logic is owned by another enterprise?

In addition to the above considerations, the following key concepts should be addressed by the Web services security recommendation:

- Authorization – Verification that an entity is allowed to perform a requested action.
- Authentication – Verification that an entity is who it claims to be.
- Integrity – Verification that the contents of a message have not been tampered with.
- Confidentiality – Ensuring that the content of a message is hidden from everyone but the intended recipient.
- Non-repudiation – Ability to correlate a message back to a specific person or entity without deniability.
- Administration and Management – Ability to manage security services for users and applications.

Regardless of the standards and approaches taken to achieve secure Web services, several key requirements must be met:



- Any security solution must conform to and support requirements set forth in the FSA *Information Technology Security and Privacy Policy*.
- An appropriate risk analysis must be performed to determine what levels of security are applicable for a given situation.
- Security requirements should be based on the sensitivity of the data involved and upon individual system dependencies.

The following sections will address Web service security standards and how they can be used to ensure security both within FSA and with trading partners.

5.1 Web Service Security Technologies and Standards

Since Web services are an emerging technology, the technologies and standards associated with securing Web services are continuing to evolve; however, this does not prohibit meeting a desired set of security objectives. Additional effort may be required to coordinate the implementation of security controls as well as new standards as they are developed and accepted by industry. The following table lists current Web services security technologies, standards, and potential applications at FSA:

Technology /Standard	Security Benefit	Description	Expected Usage
SSL/HTTPS	Confidentiality Integrity Authentication Non-repudiation	SSL is an existing TCP/IP security protocol used to secure web communication at the transport layer.	SSL can be used to encapsulate and protect Web services communications from point to point.
XML-Encryption	Confidentiality Integrity	Standard for encrypting the payload of XML SOAP messages.	Parts of an XML document can be encrypted.
XML-Signature	Integrity Authentication Non-Repudiation	Standard for generating a hash and signing XML SOAP messages.	Parts of an XML document can be digitally signed.
XKMS	Management	XML Key Management Standard - a specification that enables Web services to register and manage cryptographic keys used for digital signatures and encryption.	Thin clients can obtain key information (values, certs.) to enable secure end-to-end communications.
SAML	Authentication Authorization	SAML (Security Assertion Markup Language) is a standard for that enables the exchange of authentication and authorization information.	SAML defines assertions that authorize an entity to perform actions on part of documents.
XACML	Authorization	XACML (Access Control Markup Language) is a developing standard for defining Authorization Policy processing for SOAP Web services request.	XACML defines extensions to SAML that allow complex authorization rules.
WS-Security	Confidentiality Integrity Authentication Non-Repudiation	Web Services Security is a burgeoning standard developed by major industry players that defines how to use XML-encryption and XML-Signature standards with Web services SOAP messages.	WS-Security defines security standards, including signature.
WS-Security	All	WS-Security extensions are being	



Technology /Standard	Security Benefit	Description	Expected Usage
Extensions		developed to add improved security functionality to the WS-security standard	

Figure 5.1 - Web Services Security Standards

As some Web services security standards have yet to be finalized, it may be necessary to re-evaluate any standards choices that are made during the next 1-3 years in the event that a major shift in Web services security standards takes place. In the event that such a standards shift occurs, it may be necessary to replace some security implementations to meet the more accepted standards. The following figure illustrates the evolving state of Web services security standards:

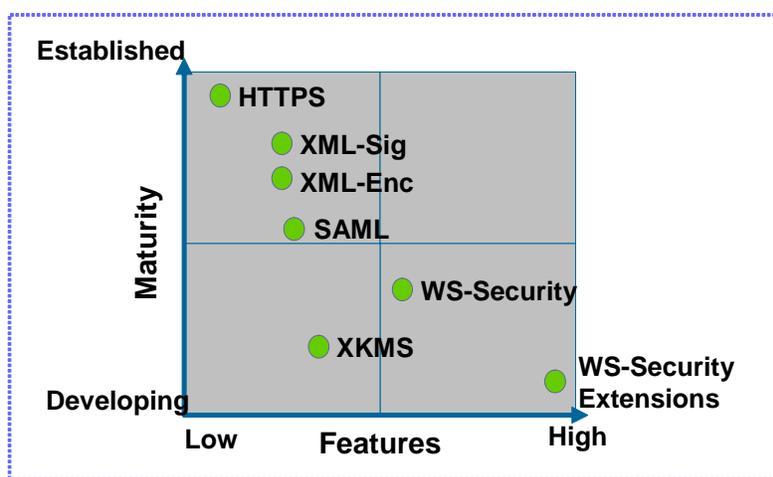


Figure 5.2 - Maturity vs. Features of Security Technologies⁴

The intent of this document is not to recommend specific standards regarding Web services security, but to provide a set of suggested criteria for when to purchase or implement systems that adhere to a specific standard or set of standards. In general, the following criteria should be applied when adopting Web services security standards:

- The standard must support required functionality.
- The maturity of the standard should be taken into account.
- The standard must be accepted by industry leaders.
- The standard must support other FSA requirements and standards.
- Products and tools must be available to support the standard.

⁴ © Accenture Security Technology Specialty, “Web Services Security Point of View”, March 2003.



5.2 *Securing Web Service Discovery*

One of the first lines of defense for preventing unauthorized access to enterprise Web services is to restrict access to UDDI repositories that provide automatic service lookup capabilities through the application of authentication services on the UDDI server. By restricting access to the UDDI lookup capabilities, the services definitions that are stored on the UDDI server are more protected.

In addition to providing authentication at the UDDI server, access controls could also be in place to limit the services that a particular user or system can discover based upon user role definitions. Access control standards for the UDDI server should be created as part of an overall enterprise Web services governance approach. Different access control levels would likely be required for external and internal Web services.

5.3 *Communication Channel Security*

More important than securing Web service discovery is ensuring the integrity of the communication channels that are being used for the transport of the Web service requests and responses. For Web service requests that take place between FSA and trading partners via the public Internet, the security of service request is of utmost importance due to privacy concerns. There must be a way to encrypt the data and determine if data has been tampered with during transport.

For Web service requests that take place within the FSA enterprise, communication channel security is not as much of a concern; however, some security may be required for sensitive data. The simplest method for ensuring communication channel security is by using SSL for data encryption. SSL is widely used and is relatively easy to implement. In addition, Virtual Private Network (VPN) connectivity or dedicated point-to-point connections between FSA and trading partners could be established to enable secure channel communications.

5.4 *User Verification, Authentication and Access Control*

Another layer of security for Web services is to verify users' identity through authentication at the time the Web service request is made. By requiring authentication at the time of Web service invocation, it will be much harder for an unauthorized person to invoke a Web service. Like the access control requirements for the UDDI repository, a set of access controls that limit the Web services that a particular user can invoke based upon role is also required. The access controls that limit invocation of individual Web services to a particular group of users should be created as part of an enterprise-wide Web services governance approach. The existing FSA requirements for user verification, authentication, and access control as set forth in the *Information Technology Security and Privacy Policy* must be adhered to.

In addition to providing authentication services for FSA resources, any authentication solution should also provide long-term support for the E-Authentication Gateway (E-AG) project that is part of the E-Gov initiative spearheaded by the Office of Management and Budget (OMB) and



the General Services Administration (GSA). The E-AG initiative seeks to provide a centralized means of authentication for government systems that will provide the following benefits⁵:

- Reduce authentication system development and acquisition costs, and reallocate labor resources used to develop such systems.
- Reduce the burden on the public in complying with repeated, duplicate or inconsistent processes of identity proofing.
- Make consistent authentication decisions.
- Promote public trust in the use of online service delivery.
- Use existing and future e-authentication processes, within their organizations or those that are available Government-wide.
- Reduce the number and type of electronic credentials that Federal employees, citizens, and businesses need to conduct business electronically with the Government.

The PIN authentication site utilizes user verification to ensure that the individual user accessing its services has permissions to do so.

5.5 Entity Verification, Authentication and Access Control

One unique challenge that is presented by Web services is ensuring that the parties participating in Web service exchange are not imposters. Two different scenarios must be protected against – systems that are posing as trusted FSA trading partners and systems that are posing as FSA. Verification of system identity can be achieved through means similar to those for verifying individual users and can include authentication methods such as shared secrets (i.e., passwords), digital certificates, tokens, and smart cards to name a few. The process for entity verification, authentication, and access control must follow those set forth in the *Information Technology Security and Privacy Policy*.

In addition to verification and authentication, access controls should be in place to limit the access a particular system or group of systems has to a given Web service or set of Web services. The entity-level access controls should be established as part of an enterprise-wide Web services governance approach. The PIN authentication site utilizes entity verification to ensure that the calling system has permissions to invoke the PIN authentication service.

⁵ *Federal Register*, Vol. 68, No. 133, 11 July 2003, “Notices”



6 Recommendation

The following sections provide a recommendation for the FSA Web Services Strategy. This recommendation required consideration of FSA business needs, industry trends, and an understanding of the potential return on investment. The rationale for considering the use of Web services at FSA focuses on the following:

- Bridging gaps that were identified by FSA.
- Meeting FSA's business objectives.
- Enabling FSA's key decision factors.
- Achieving the desired benefits of:
 - Improving operational efficiencies.
 - Promoting reuse of business functionality.
 - Increasing the self-service capabilities.
 - Driving integration procedures that best align with business processes.

This recommendation is only one portion of the overall Data Strategy and it takes into consideration FSA cross-lifecycle business processes. The Web Services Strategy requires a thorough understanding of all the components that go into the Data Strategy effort in order to realize its full business value. This "big think" approach helps to ensure that a solution option has acceptable trade-offs across all of FSA. It should be noted that no single solution fits all requirements, and furthermore the implementation of a new strategy and architecture requires a carefully planned and iterative approach.

The recommendation below builds off the analysis of the technical options examined above and their ability to help FSA achieve its overall business goals, fill outlined gaps and integrate with an overall data vision. Web services are a key component of FSA's overall strategy as they enable a uniform way to integrate disparate systems and processes across the enterprise.

6.1 Recommendation Summary

Web services technology has matured and the industry is accepting Web services as an efficient method of sharing information and exchanging data, while providing valuable business capabilities across the enterprise and to external customers. Based on the evaluation of the key decision questions, the following strategy for Web services is recommended for FSA to reach its target state and achieve its business objectives:

- Leverage Web services to allow standard access to system look-up capabilities.
- Integrate Web services technology with the Web Usage Framework to provide access to business capabilities through the Portals.
- Apply Web services security standards to protect access to FSA business capabilities.
- Couple Web services with Business Process Management to enable business capabilities requiring multi-system coordination.
- Enable Web service discovery via a common repository of Web service capabilities.



-
- Engage a standard governance structure to oversee the implementation for both internal and external Web services.

By utilizing Web services, FSA can:

- Provide the capability for students and trading partners to use services through common standard user tools.
- Provide a common integration technique for both internal FSA systems and external trading partner systems that are involved in the financial aid process.
- Provide the capability to deploy cross-lifecycle interfaces where it was previously too complicated and too costly to implement.

6.1.1 How will Web services promote integration of business capabilities?

FSA should take an iterative approach to developing the capability to integrate its business functions via Web services. In the beginning, emphasis should be placed on implementing simple business services that can provide the most value to its customers. Significant business value can come from providing access to Web services through the Web. This provides a tangible solution to customer requests for information and gives the user increased capabilities for self-service.

Through deeper interaction with the integration platform, FSA could provide more complex services that bring comprehensive business functions to the end users. Great benefits would come through leveraging the business process management capabilities of the integration platform that could enable an organization to retrieve and share data contained in FSA's systems. The XML Framework, as it is envisioned, will provide the technical foundations for standardizing data exchange, as FSA proceeds with implementations recommended by the Data Strategy Enterprise-Wide initiative.

The implementation of Web services at FSA should build upon the concepts of the XML Framework team's recommendation since XML is the foundation for enabling Web services. As more business services are enabled through Web services, the use of XML across the enterprise will increase. FSA should leverage the principles outlined by the XML Framework team and utilize the XML Core Component definitions for developing new data exchange interfaces. For more information on the XML Framework, refer to the XML Framework Strategic Assessment and Enterprise Vision (123.1.13).

To realize the full benefits of Web services over time and achieve FSA's business objectives, the iterative approach to implementing Web services capabilities should follow three key steps 1) Think Big, 2) Start Small and 3) Build Out. This process is illustrated in the diagram below:

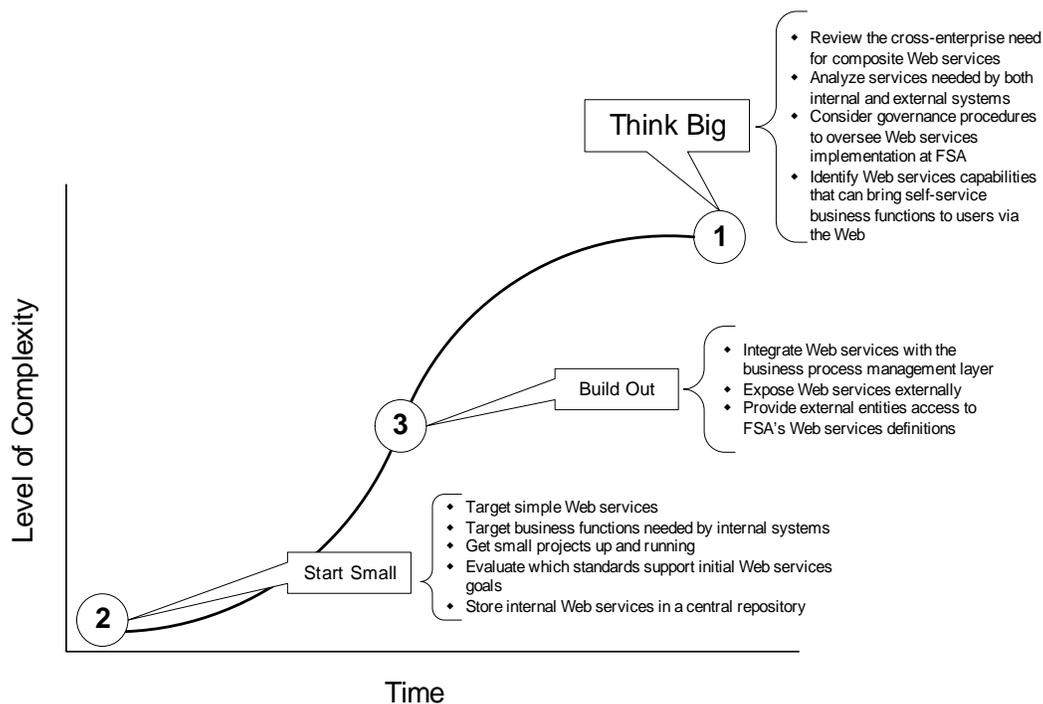


Figure 6.1 - Evolutionary Approach to Web Services

Initially, FSA should look to implement Web services for simple business functions such as look-up capabilities and common calculations. A simple Web service would target information that resides in a single location but is needed by multiple systems within the enterprise. This strategy references the EFC calculator as an example of a simple Web service.

FSA can expand its use of Web services by sharing business functions with systems that are external to FSA. With internal Web services in place and continuing to evolve, FSA should move to the second stage and provide access to certain simple Web services to its trading partners' systems. For example, schools could connect their systems to the EFC Web service to offer this business capability to their students who are entering the financial aid process.

The third and fourth stages of a phased implementation involve increasing the complexity of Web services to bring composite business capabilities to internal and external systems. A composite Web services could leverage the integrated services layer of FSA's middleware technology to enable business services that could be leveraged by both internal and external systems.

By enabling delivery of business functions to multiple systems and providing users with better access to information, the enterprise can realize the following benefits:

- Sharing services across applications, channels, departments and agencies.
- Optimizing and streamlining processes.



- Automating current processes.
- Leveraging existing infrastructure.
- Reaching a larger customer base.
- Reducing time of delivery.

6.1.2 How will Web services be communicated and managed?

Once FSA begins to implement Web services, the organization should take a uniform approach to service discovery and governance. Web service discovery is needed to provide a method for locating and accessing FSA business services. FSA should enable Web service discovery via a common UDDI repository of Web service capabilities. The discovery mechanisms should be used as a means of communicating to both the internal FSA community as well as to the external trading partners. Sharing discovery services to the external community requires secure methods of enabling access to the information contained in the repository. FSA should look to enable Web services discovery externally (as needed) after successfully implementing an internal discovery mechanism. This iterative approach supports the recommendation of a phased implementation of internal and external Web services.

In addition to Web service discovery, a consistent and centralized approach to enterprise Web services governance must be taken to ensure the successful deployment and implementation of enterprise-level Web services at FSA. The approach to enterprise Web services governance should be addressed before the first Web service is deployed to ensure that all FSA Web services meet the same requirements. At a minimum, the governance procedures should aid FSA in evaluating the proposed functionality against the following criteria:

- Satisfies a need for mass accessibility to a common functionality.
- Replaces duplicative functionality across multiple systems.
- Is compatible with the existing architecture.
- Supports current business processes.
- Enables low volume transactions.

6.1.3 How will Web services be secured?

Even though standards for securing Web services are still evolving, the technology has grown to a point that Web services can be properly secured and successfully implemented. Because Web services are based on Internet standards, many of the security challenges can be handled by leveraging existing Web security concepts with emerging standards.

Security can be applied to Web services at different levels. For example, the UDDI repository can employ access control mechanisms to prevent unauthorized access to Web service discovery. The transport layer of Web services messages can also have security controls that protect the communication between systems. As standards mature, the manner in which transport, data and authentication are secured will become uniform across systems, requiring less effort to communicate securely with partners. A set of criteria for adopting Web services security standards should be established.



6.2 Recommendation Benefits

There are numerous business processes and technological benefits associated with utilizing enterprise-level Web services. The potential cost savings associated with these benefits is particularly important for government agencies:

- Increased Operational Efficiency and Quality of Service.
 - Increased accuracy of information gathered through reducing the human error factor.
 - Increased ability to collect data once and distribute it across many government departments and agencies.
 - Increased efficiency through the automation of existing processes.
 - Improved employee performance and productivity, which enables employees to focus more on higher value services.
- Improved Return on Investment.
 - Reduced cost associated with sustaining existing legacy capabilities while lowering the cost of integrating new capabilities.
 - Increased cost savings through the reduction of manual transaction processing.
 - Faster low-cost, low-risk and platform-neutral system integration and development.
- Provides a Flexible and Agile Infrastructure.
 - Improved consistency across internal organizations and government agencies.
 - Allows for planned replacement of legacy systems while improving service to constituents.
 - Ability to add new services easily and cost effectively while leveraging and reusing existing IT capabilities.
 - Enables the ability for systems to be easily added to or removed from the architecture.

Finally, Web services support broader eGovernment initiatives that promote citizen access to government services. The General Services Administration (GSA) reviewed the importance of Web services as an emerging technology. Its analysis concluded that Web services are important to government managers because “Current e-government strategy calls for a citizen-centric government built around services rather than government bureaucracy, which requires an architecture that enables the dynamic sharing of services.”⁶

⁶ © General Services Administration, “Web Services: Using the Internet as a Shared Service Platform.” May 2002. <http://xml.gov/documents/completed/webservices.htm>



6.3 Bridging the Gaps

The following table illustrates how this overall recommendation fills the gaps as derived from the overall Web services business objectives:

Business Objective Rank	Gap Description	Fulfilled by Recommendation	Explanation
1	No means to enable common access to customer status.	✓	Web services combined with the process rules established at the business process management layer of the integrated services platform can retrieve cross-lifecycle customer status.
	No externally communicated Web services.	✓	After establishing internal Web service capabilities, FSA will be in a better position to communicate and expose certain business capabilities to external parties.
2	No common calculations enabled via Web service	✓	Web services can enable common calculations and share the logic to systems that need access to it.
	Some look-up and update capabilities exist but none are standard, centralized or using Web services.	✓	Web services can standardize look-up capabilities so multiple systems can have access to data in a consistent way.
3	PIN authentication Web Service is in place, but not utilized.	✓	Web services can be used to provide authentication services. Authentication Web services require collaboration with the PIN Re-Engineering effort.
	Security model is not in place to support service.	✓	The Security Architecture team is creating a recommendation for a security model at FSA. Supporting the recommendations outlined in this strategy, FSA should adopt Web services security standards that conform to new/existing security policies at FSA.



Business Objective Rank	Gap Description	Fulfilled by Recommendation	Explanation
	A diverse set of authentication functionality being utilized.	N/A	Authentication functionality will be outlined in the recommendations made by the Security Architecture team.
4	Limited pre-population functionality exists for the FAFSA (Free Application for Federal Student Aid) but does not leverage any Web services.	✓	Web services can be used to retrieve information from multiple systems and be used by another system to pre-populate forms.

Table 6.1 - Recommendation Gap Bridging

6.4 Alignment with Business Objectives

Fundamentally, technology that improves business process makes sense. However, it is the realization of the business value that supports change from the status quo. The matrix below reviews each of the previously defined FSA Web services business objectives. Although an assessment of the gaps should help ensure that the business objectives are reasonably met, a specific review of the business objectives is outlined below to ensure the true business needs are enabled by the strategy recommendations. Explanations of the assessment criteria can be found in Appendix A: Business Objective Accommodation Criteria.

Rank	Business Objective	Objective Fulfilment	Explanation
1.	Provide access to customer status via centralized means.		<ul style="list-style-type: none"> Web services can provide uniform access to a customer’s status for multiple systems, internal and external to FSA. A customer status Web service would leverage the business process capabilities supported by the integrated services of FSA’s Internal Data Exchange platform to provide access.
2.	Provide access to common calculations as well as lookup and update (corrections) capabilities in a standardized and central location.		<ul style="list-style-type: none"> Web services can provide look-up and common calculation capability. Web services enable a standardized format for performing common calculations and lookup capabilities that can be shared with multiple systems. Web services can uniformly distribute functionality across the enterprise from a centralized location.



**Data Strategy Enterprise-Wide
Technical Strategies
Web Services Strategy**

Rank	Business Objective	Objective Fulfilment	Explanation
3.	Enable Authentication capabilities via Web Service.		<ul style="list-style-type: none"> • Web services can enable authentication capabilities but this objective is broader than the scope of Web services alone. • Whatever mechanisms that are put in place to support authentication services must be in line with FSA's IT Security and Privacy Policy. • Authentication considerations must take into account ongoing efforts, such as the work by the PIN Re-Engineering and Security Architecture teams.
4.	Enable a pre-population of FSA Web forms using Web Services and leveraging information already gathered regarding a customer.		<ul style="list-style-type: none"> • Can be enabled through a composite Web service that collects and shares information from multiple systems. • Requires the interaction with business process rules to retrieve the data. • Needs support from the data architecture to leverage data collection techniques and information gathered on a customer.

Table 6.2 - Recommendation Business Objective Fulfillment



Appendix A – Business Objective Accommodation Criteria

The table below provides a rating scale that explains the measures and criteria used to evaluate how well a particular technical solution satisfies FSA’s business objectives. These indicators appear in the Executive Summary and Recommendation sections with respect to both the current and the recommended states for the Web Services Strategy.

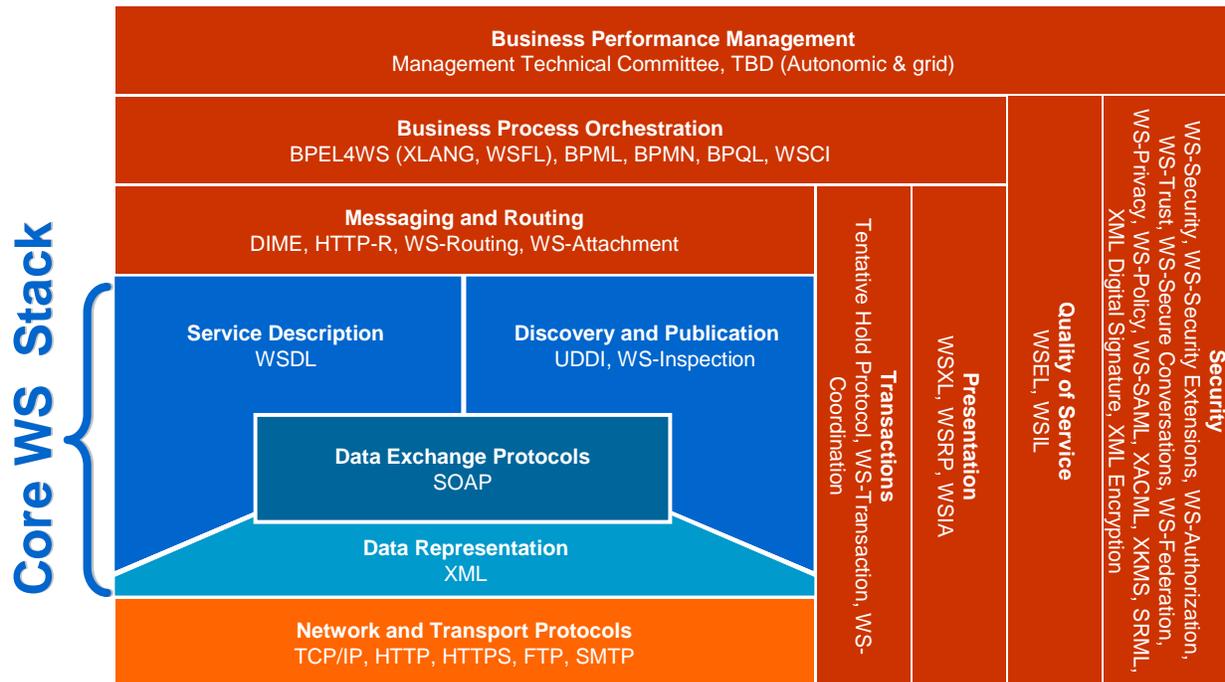
Rating Indicator	Synopsis	Criteria
	Fully Accommodated Objective	The business objective is being completely satisfied.
	Well Accommodated Objective	The business objective is mostly satisfied.
	Partially Accommodated Objective	Some business objective criteria in place, but the business objective is only partially fulfilled.
	Minimally Accommodated Objective	Few parts of the business objective are satisfied.
	Capability Not Accommodated	The solution does not have this element in place and the business objective is not met.

Business Objective Accommodation Criteria



Appendix B - Web Services Standards

The following framework contains commonly used Web services standards. Descriptions of select standards can be found below.



Web Services Framework and Standards⁷

Standard	Stack	Definition
SOAP: Simple Object Access Protocol	Information Exchange	Collection of XML-based technologies, defines an envelope for Web Service Communications, that can be mapped to HTTP and other protocols, and provides a serialization format for transmitting XML documents over a network and convention for representing Remote Procedure Call (RPC) interaction SOAP Attachments: allows SOAP message to be sent within a MIME envelope with attachments to linked from the SOAP envelop
WSDL: Web Services Description Language	Description	Defines Web services interfaces, data and message types, interaction patterns and protocol mappings
UDDI: Universal Description,	Discovery and Publication	WS registry and discovery mechanism used for storing and categorizing business information and retrieving pointers to WS

⁷ Accenture Web Services Point of View, March 2003.



**Data Strategy Enterprise-Wide
Technical Strategies
Web Services Strategy**

Standard	Stack	Definition
Discovery, and Integration		interfaces
WS-Inspection	Discovery and Publication	Microsoft/IBM proposal that defines a method to discover and locate a list of Web Services published at a particular known receiver's address.
DIME: Direct Internet Message Encapsulation	Enhanced Messaging	Format, co-developed by IBM and Microsoft, for sending multipart messages and its main purpose is to provide a way to package a SOAP message with one or more attachments
HTTP-R: Reliable Hypertext Transport Protocol	Enhanced Messaging	Allows SOAP messages between sender and receiver pairs by persisting information about the message and correlates acknowledgements and replies with original requests.
WS-Routing	Enhanced Messaging	A simple, stateless, SOAP-based protocol for routing SOAP messages in an asynchronous manner over a variety of transports like TCP, UDP, and HTTP supporting one-way messaging, two-way messaging (such as request/response and peer-to-peer conversations), and long running dialogs. With WS-Routing, the entire message path for a SOAP message (as well as its return path) can be described directly within the SOAP envelope.
WS-Attachment	Enhanced Messaging	A draft specification describes an abstract model for SOAP messages to include attachments as well as encapsulating a SOAP message and its attachments within a DIME message.
Tentative Hold Protocol	Transaction	Open, loosely coupled messaging-based protocol for the exchange of information across businesses prior to an actual transaction, recognizing the extremely dynamic nature of business conditions originally developed by Intel.
WS-Coordination	Transaction	Framework that enables application services to create a context needed to propagate an activity to other services, register for coordination protocols and provide a method to coordinate the isolation of proprietary protocols in order to operate in a heterogeneous environment.
WS-Transaction	Transaction	Consists of two coordination types within the WS-Coordination framework: <ul style="list-style-type: none"> • Atomic Transaction (AT): Coordinates activities having a short duration and executed within limited trust domains • Business Activity (BA): Coordinates activities that are long in duration and desire to apply business logic to handle business exceptions
WSXL (Web	Presentation	A component model for interactive Web applications designed to



**Data Strategy Enterprise-Wide
Technical Strategies
Web Services Strategy**

Standard	Stack	Definition
Services Experience Language)		achieve two main goals: enable businesses to distribute Web applications through multiple revenue channels and enable new services or applications to be created by leveraging existing applications across the Web
WSRP (Web Services for Remote Portals)	Presentation	This specification describes visual, user-facing Web Services-centric components that plug-n-play with portals or other intermediary web applications that aggregate content or applications from different sources. Designed to enable businesses to provide content or applications in a form that does not require any manual content- or application-specific adaptation by consuming intermediary applications.
WSIA (Web Services for Interactive Applications)	Presentation	A framework for interactive web applications designed to enable businesses to distribute web applications through multiple revenue channels and enable new services or applications to be created by leveraging existing applications across the Web.
WSEL (Web Services Endpoint Language)	Quality of Service	An XML format for the description of non-operational characteristics of service endpoints, like quality-of-service, cost or security properties.
WSIL (Web Services Inspection Language)	Quality of Service	Defines how a service requestor can discover an XML Web Service description on a Web server, enabling such requestors to easily browse Web servers for XML Web Services.
BPEL4WS: Business Process Execution Language for WS	Business Process Orchestration	Specification for a programming language that enables a task to be accomplished using a combination of Web Services. Developed by BEA Systems, IBM, and Microsoft, BPEL4WS combines and replaces IBM's Web Services Flow Language (WSFL) and Microsoft's XLANG specification
BPML: Business Process Modeling Language	Business Process Orchestration	XML-based meta-language developed by the Business Process Management Initiative (BPMI) as a means of modeling business processes, much as XML is a meta-language with the ability to model enterprise data. BPMI has also defined Business Process Modeling Notation (BPMN) and Business Process Query Language (BPQL).
WSCSI (Web Services Choreography Interface)	Business Process Orchestration	XML-based interface description language that describes the flow of messages exchanged by a Web Service participating in choreographed interactions with other services (initiative from SAP, BEA, Sun and Intalio)
WS-Security	Security	A model for many levels of security needed for services. It includes enhancements to SOAP to provide quality of protection



**Data Strategy Enterprise-Wide
Technical Strategies
Web Services Strategy**

Standard	Stack	Definition
		mechanisms, a general-purpose mechanism to associate security-tokens with messages, and describes how to encode binary security tokens in messages.
WS-Authorization	Security	Defines how Web Services manage authorization data and policies
WS-Policy	Security	Defines how to express the capabilities and constraints of security policies
WS-Trust	Security	Describes the model for establishing both direct and brokered trust relationships (including third parties and intermediaries)
WS-Privacy	Security	Defines how Web Services state and implement privacy practices
WS-Secure Conversation	Security	Describes how to manage and authenticate message exchanges between parties, including security context exchange and establishing and deriving session keys
WS-Federation	Security	Describes how to manage and broker trust relationships in a heterogeneous federated environment, including support for federated identities
WS-Security Extensions	Security	Clarifies elements released in the original document and introduces some new items including timestamps, and passing around passwords and security certificates.
WS-SAML	Security	Defines a general framework to enable XML-based security tokens to be used with WS-Security. Two profiles that use this general framework are provided: one for the Security Assertion Markup Language (SAML) and other for the eXtensible rights Markup Language
XACML	Security	Defines an XML specification for expressing policies for information access over the Internet .
XKMS	Security	XML Key Management Specification specifies protocols for distributing and registering public keys, suitable for use in conjunction with the proposed standard for XML Signatures.
SRML	Security	Simulation Reference Markup Language: markup language for representing behavior in XML. SRML enables both the structure and behavior of XML documents to execute on the World Wide Web or other distributed environment.
XML Digital Signature	Security	XML Digital Signature specifies XML syntax and processing rules for creating and representing digital signatures.



**Data Strategy Enterprise-Wide
Technical Strategies
Web Services Strategy**

Standard	Stack	Definition
XML Encryption	Security	This specification provides requirements for a XML syntax and processing for encrypting digital content, including portions of XML documents and protocol messages.
Management Technical Committee	Management	Develop open industry standard management protocols to provide a web-based mechanism to monitor and control managed elements in a distributed environment based on industry accepted management models, methods, and operations, including, OMI, XML, SOAP, DMTF CIM, and DMTF CIM Operations
TBD (Autonomic & grid)	Management	Grids provide access to heterogeneous and geographically distributed applications, data, processing power, storage capacity and a vast array of other computing resources over a network, using a set of open standards and protocols. Autonomic computing assist in the reduction the complexity from a growth of volumes. Grid and autonomic computing are being developed in order to provide reliable and efficient, self-managing Grids

Web Services Standards



Appendix C: Meeting Minutes – Working Session #1

Date: Wednesday, 08/06/2003

Time: 2:00 – 4:00 PM

Location: 221C

Objectives: The objectives of the first working session were to review options for the Web Services Strategy and to decide upon an option or combination of options that will best meet FSA’s future needs.

Attendees:

Name	Business/System Area	E-Mail	Phone (Work)	Attendance
Jesse Bowen	Integration Partner	Jesse.w.bowen@accenture.com	202.962.0744	X
Roger Hartmuller	Integration Partner	Roger.l.hartmuller@accenture.com	202-962-4160	X
Denise Hill	FSA/CIO	Denise.hill@ed.gov	202.377.3030	X
Corwin Jennings	Ombudsman	Corwin.jennings@ed.gov	202.377.3291	X
Kyle Michl	Integration Partner	Kyle.a.michl@accenture.com	202.962.0750	X
Robert O’Keefe	Integration Partner	Robert.f.okeefe@accecnture.com	703.587.8652	X
Davis Peden	Integration Partner	Davis.w.peden@accenture.com	202.962.0651	X
Ganesh Reddy	FSA/CIO	ganesh.reddy@ed.gov	202.377.3557	X
Merlina Rigo	Financial Partners	Merlino.Rigo@ed.gov	202-377-3352	Phone
Marty Winslow	EDS	Marty.winslow@ed.gov	202-377-3023	Phone
Terry Woods	FSA/CIO	Terry.woods@ed.gov	202-377-3023	X

Action Items from Previous Meeting Minutes

N/A

Discussion Points

The meeting opened with a review of the status with respect to the Technical Strategies Roadmap. The meeting agenda and working session goals were also covered.

Concern was raised over whether or not attendance for the meeting was sufficient. It was agreed, that another meeting might need to take place.

The definition of Web services with respect to FSA was discussed. The group agreed that the definition as presented at the top of the Key Decisions matrix was sufficient to meet FSA’s needs; however, the group asked that the definition also include a reference to Web services being “location agnostic”.

Emphasis was placed on the Web Services Strategy needing to include both near-term and long-term considerations.



Concern was raised over the transaction volumes that Web services can handle. The group agreed that latency and overall interface performance must be taken into account for Web services. Web services can be used where there is no real or perceived impact to performance.

KEY DECISION SUMMARY

No.	Key Decision(s)	Options	Potential Solution
Ext. Web Svcs.	a. What criteria should be used when identifying an internal Web service candidate?	<ul style="list-style-type: none"> • High potential for service reuse by internal systems. • Increased levels of business logic consolidation. • More... 	<ul style="list-style-type: none"> • No real or perceived impact to performance. • Services should support both synchronous and asynchronous transactions. • Low-volume batch is acceptable. • Must have clearly defined and logical units of work. • Consumer application's needs must be met. • Support of current business processes in a distributed manner.
	b. What functionality exists that could be enabled as an internal Web service today? What functionality could be enabled in the future?		<ol style="list-style-type: none"> 1. EFC Calculator. 2. Common data access/update. 3. Student eligibility checks (CPS, FAFSA, COD). 4. PIN Matching. 5. PLUS Credit Check. 6. Financial Transaction Updates (Principle balance update, interest change update, update to original transactions). 7. Status Information on Consolidation – ECMO. 8. Promissory note images.



**Data Strategy Enterprise-Wide
Technical Strategies
Web Services Strategy**

No.	Key Decision(s)	Options	Potential Solution
	c. What standards will be applied to internal Web services?	<ul style="list-style-type: none"> • HTTP – HyperText Transfer Protocol. • HTTPS – Secure HyperText Transfer Protocol. • SOAP - Simple Object Access Protocol - a lightweight XML based protocol for exchange of information in a decentralized, distributed environment. • XML - Extensible Markup Language is a simple, very flexible text format derived from Standard Generalized Markup Language (SGML). • UDDI – Universal Description, Discovery and Integration – a mechanism for Web service providers to advertise the existence of their Web services and for the consumers to locate them. • WSDL – Web Service Description Language – describes the components necessary to call a particular Web service. 	<ul style="list-style-type: none"> • All standards are ok for internal web services.
	d. How will internal Web services be “discovered”?	<ul style="list-style-type: none"> • Web services not published. • Manual communication. • Web site distribution (i.e., downloads). • UDDI repository. 	<ul style="list-style-type: none"> • Internal UDDI repository is preferred method. • Consideration must be given to centralized management and governance of Web services within the enterprise.
Int. Web Svcs.	a. What criteria should be used when identifying an external Web service candidate?	<ul style="list-style-type: none"> • High potential for service reuse by external partners. • Increased levels of business logic consolidation. • More... 	<ul style="list-style-type: none"> • Same criteria apply from internal.
	b. What functionality exists that could be enabled as an external Web service today? What functionality could be enabled in the future?		<ol style="list-style-type: none"> 1. EFC Calculator. 2. FAFSA Status Lookup. 3. Financial Aid Status. 4. Promissory note lookup – people need to know when they expire. 5. Loan Consolidation Status. 6. School information correction. 7. Faster updates to ISIRs. 8. IRS Checks (dependent on IRS capabilities). 9. Congressional Lookup Capability.



**Data Strategy Enterprise-Wide
Technical Strategies
Web Services Strategy**

No.	Key Decision(s)	Options	Potential Solution
	c. What standards will be applied to external Web services?	<ul style="list-style-type: none"> • HTTP – HyperText Transfer Protocol. • HTTPS – Secure HyperText Transfer Protocol. • SOAP - Simple Object Access Protocol - a lightweight XML based protocol for exchange of information in a decentralized, distributed environment. • XML - Extensible Markup Language is a simple, very flexible text format derived from Standard Generalized Markup Language (SGML). • UDDI – Universal Description, Discovery and Integration – a mechanism for Web service providers to advertise the existence of their Web services and for the consumers to locate them. • WSDL – Web Service Description Language – describes the components necessary to call a particular Web service. 	<ul style="list-style-type: none"> • All standards were uniformly accepted with the exception of UDDI and WSDL. • Security considerations must be made around using UDDI in a public-facing manner. • Care should be taken when distributing WSDLs to ensure the highest levels of security. • Authentication must be used during Web service calls so ensure that services are invoked only by users who have sufficient privileges.
	d. How will external Web services be “discovered”?	<ul style="list-style-type: none"> • Web services not published. • Manual communication. • Web site distribution (i.e., downloads). • UDDI repository. 	<ul style="list-style-type: none"> • Security risk profile of the service needs to be appropriate to support certain transactions. • Need to allow external partners to see that services pertaining to them exist without exposing all services available. • Secure discovery in an automated fashion is preferred.

New Action Items

Action Item	Owner	Date Due
Update Key Decisions Matrix with content from this meeting in order to facilitate working session #2.	Technical Strategies Team	8/12/2003
Email Web services definitions and security requirements to Technical Strategies Team	Meeting Attendees	8/12/2003

Next Meeting Time

Tuesday, August 12, 2003 – 3:00 until 5:00pm room 221C

Suggested Agenda Items

None at this time.



Appendix D: Meeting Minutes – Working Session #2

Date: Tuesday, 08/12/2003

Time: 3:00 – 5:00 PM

Location: 221C

Objectives: The objectives of the second working session were to review options for the Web Services Strategy and to decide upon an option or combination of options that will best meet FSA’s future needs.

Attendees:

Name	Business/System Area	E-Mail	Phone (Work)	Attendance
Jackie Anderson	FP	Jackie.anderson@ed.gov	202.377.3315	X
Jesse Bowen	Integration Partner	Jesse.w.bowen@accenture.com	202.962.0744	X
Emanuel Bundy	FP	Emanuel.bundy@ed.gov	202.377.3316	X
Denise Hill	FSA/CIO	Denise.hill@ed.gov	202.377.3030	X
Sandra Fowler	FP	Sandra.fowler@ed.gov	202.377.3549	X
Terry Hardgrave	Pearson/CIO	Terry.hardgrave@ed.gov	202.377.3238	X
Holly Hyland	Title IV Delivery	Holly.hyland@ed.gov	202.377.3710	X
Corwin Jennings	Ombudsman	Corwin.jennings@ed.gov	202.377.3291	X
Kyle Michl	Integration Partner	Kyle.a.michl@accenture.com	202.962.0750	X
Davis Peden	Integration Partner	Davis.w.peden@accenture.com	202.962.0651	X
Marty Winslow	EDS	Marty.winslow@ed.gov	202-377-3023	Phone
Terry Woods	FSA/CIO	Terry.woods@ed.gov	202-377-3023	X

Action Items from Previous Meeting Minutes

Key Decisions Matrix updated with content from last meeting.

Web services definition and security considerations were emailed to the Technical Strategies Team.

Discussion Points

The meeting opened with a re-cap of the previous week’s first working session. This working session is intended to supplement the material that was captured from the first session.



KEY DECISION SUMMARY

No.	Key Decision(s)	Options	Potential Solution
Ext. Web Svcs.	a. What criteria should be used when identifying an internal Web service candidate?	<ul style="list-style-type: none"> • High potential for service reuse by internal systems. • Increased levels of business logic consolidation. • More... 	<ul style="list-style-type: none"> • No real or perceived impact to performance. • Services should support both synchronous and asynchronous transactions. • Low-volume batch is acceptable. • Must have clearly defined and logical units of work. • Consumer application's needs must be met. • Support of current business processes in a distributed manner. • Web services should be compatible with existing architecture. • Composite functions across multiple systems.
	b. What functionality exists that could be enabled as an internal Web service today? What functionality could be enabled in the future?		<ol style="list-style-type: none"> 1. EFC Calculator. 2. FAFSA Status Lookup. 3. Financial Aid Status. 4. Promissory note lookup – people need to know when they expire. 5. Loan Consolidation Status. 6. School information correction. 7. Faster updates to ISIRs. 8. IRS Checks (dependent on IRS capabilities). 9. Congressional Lookup Capability. 10. Lender and Guarantor Lookups 11. Financial Partners Form 2000 12. Status of action taken on accounts - Ombudsman



**Data Strategy Enterprise-Wide
Technical Strategies
Web Services Strategy**

No.	Key Decision(s)	Options	Potential Solution
	c. What standards will be applied to internal Web services?	<ul style="list-style-type: none"> • HTTP – HyperText Transfer Protocol. • HTTPS – Secure HyperText Transfer Protocol. • SOAP - Simple Object Access Protocol - a lightweight XML based protocol for exchange of information in a decentralized, distributed environment. • XML - Extensible Markup Language is a simple, very flexible text format derived from Standard Generalized Markup Language (SGML). • UDDI – Universal Description, Discovery and Integration – a mechanism for Web service providers to advertise the existence of their Web services and for the consumers to locate them. • WSDL – Web Service Description Language – describes the components necessary to call a particular Web service. 	<ul style="list-style-type: none"> • All standards were uniformly accepted with the exception of UDDI and WSDL. • Security considerations must be made around using UDDI in a public-facing manner. • Care should be taken when distributing WSDLs to ensure the highest levels of security. • Authentication must be used during Web service calls so ensure that services are invoked only by users who have sufficient privileges. • Note that BEPL was added for consideration following the first working session. • In second working session, it was agreed that process coordination is required for Web services. Initially this will be fulfilled by BEPL.
	d. How will internal Web services be “discovered”?	<ul style="list-style-type: none"> • Web services not published. • Manual communication. • Web site distribution (i.e., downloads). • UDDI repository. 	<ul style="list-style-type: none"> • Security risk profile of the service needs to be appropriate to support certain transactions. • Need to allow external partners to see that services pertaining to them exist without exposing all services available. • Secure discovery in an automated fashion is preferred. • In second working session, it was agreed that UDDI would be used for external Web service discovery with proper security and access controls in place. • Notices that Web services exist should be posted in the form of FAQs to notify the trading partner community that services exist.



**Data Strategy Enterprise-Wide
Technical Strategies
Web Services Strategy**

No.	Key Decision(s)	Options	Potential Solution
Int. Web Svcs.	a. What criteria should be used when identifying an external Web service candidate?	<ul style="list-style-type: none"> • High potential for service reuse by external partners. • Increased levels of business logic consolidation. • More... 	<ul style="list-style-type: none"> • No real or perceived impact to performance. • Services should support both synchronous and asynchronous transactions. • Low-volume batch is acceptable. • Must have clearly defined and logical units of work. • Consumer application's needs must be met. • Support of current business processes in a distributed manner. • Web services should be compatible with existing architecture. • Composite functions across multiple systems.
	b. What functionality exists that could be enabled as an external Web service today? What functionality could be enabled in the future?		<ol style="list-style-type: none"> 1. EFC Calculator. 2. Common data access/update. 3. Student eligibility checks (CPS, FAFSA, COD). 4. PIN Matching. 5. PLUS Credit Check. 6. Financial Transaction Updates (Principle balance update, interest change update, update to original transactions). 7. Status Information on Consolidation – ECMO. 8. Promissory note images. 9. Error visibility – ability to see errors as they occur across multiple systems. 10. Data integrity checker. 11. CSB Student Status Lookup. 12. Client/Partner management views – ability to monitor all entry points into FSA.



**Data Strategy Enterprise-Wide
Technical Strategies
Web Services Strategy**

No.	Key Decision(s)	Options	Potential Solution
	c. What standards will be applied to external Web services?	<ul style="list-style-type: none"> • HTTP – HyperText Transfer Protocol. • HTTPS – Secure HyperText Transfer Protocol. • SOAP - Simple Object Access Protocol - a lightweight XML based protocol for exchange of information in a decentralized, distributed environment. • XML - Extensible Markup Language is a simple, very flexible text format derived from Standard Generalized Markup Language (SGML). • UDDI – Universal Description, Discovery and Integration – a mechanism for Web service providers to advertise the existence of their Web services and for the consumers to locate them. • WSDL – Web Service Description Language – describes the components necessary to call a particular Web service. 	<ul style="list-style-type: none"> • All standards are ok for internal web services • Note that BEPL was added for consideration following the first working session. • In second working session, it was agreed that process coordination is required for Web services. Initially this will be fulfilled by BEPL.
	d. How will external Web services be “discovered”?	<ul style="list-style-type: none"> • Web services not published. • Manual communication. • Web site distribution (i.e., downloads). • UDDI repository. 	<ul style="list-style-type: none"> • Internal UDDI repository is preferred method. • Consideration must be given to centralized management and governance of Web services within the enterprise.

New Action Items

Action Item	Owner	Date Due
None identified.		

Next Meeting Time

To be announced.

Suggested Agenda Items

None at this time.