

# Manufacturing the PERFECT MORTGAGE: An INNOVATION Challenge

---

## THOUGHT PAPER ON Data Format and Transmission Management

---

Integration and Distribution Innovation Challenge Team

***Data Format and Transmission Management Sub Committee Team Members:***

Darius Bozorgi – Veros, Team Chair  
Richard Ching – Veros, Lead for Paper  
Trevor Davies – DataVerify  
Don Smith – RealEC  
Einat Haftel – Informatica  
Joe Palese – Federal Home Loan Bank of Chicago  
Tom Terpstra – Federal Home Loan Bank of Chicago  
Ginger Ricchetti – Regions

***Additional Contributors***

Anna Warner – Veros  
Jim Blust – Veros  
Justin Leiser – Fannie Mae  
Kristin Hoffman – Fannie Mae  
Phung Le – Veros

January 17, 2014, Version 1.13



## Table of Contents

1	Executive Summary .....	4
2	Overview .....	5
	2.1 Introduction.....	5
	2.2 Objective and Scope .....	5
3	Approach.....	5
	3.1 Survey.....	6
	3.2 Survey Response Categories .....	6
	3.3 Level of Integration .....	7
4	Analysis and Scoring .....	8
	4.1 Scoring.....	8
	4.2 Integration Components Analysis .....	8
	4.2.1 User Security (Authentication and Authorization) .....	8
	4.2.2 Message Security (Integrity and Confidentiality).....	10
	4.2.3 Quality of Service (Reliability and Transactions) .....	11
	4.2.4 Multi-Party Quality of Service.....	14
	4.3 Other Considerations Analysis .....	15
	4.3.1 Data Formats and Data Definitions.....	15
	4.3.2 Payload Efficiency .....	16
	4.3.3 Caching.....	16
	4.3.4 Multiple Representations of Data.....	17
	4.3.5 Message Transport Options.....	17
	4.3.6 Synchronous and Asynchronous Services.....	18
	4.3.7 Formal Service Specifications .....	19
	4.3.8 Industry Standard Tools and Support .....	20
5	Analysis Summary .....	21
6	Recommendations.....	22
	6.1 Current SOAP Integrations .....	22
	6.2 New SOAP Integrations .....	22
7	Strategy for Legacy Integrations.....	23
8	Next Steps.....	23



- 9 Appendix..... 24
  - 9.1 Appendix A – Glossary of Terms..... 24
  - 9.2 Appendix B – Detailed Survey Results..... 26
  - 9.3 Appendix C – Web Service Architecture Comparison ..... 31



## 1 EXECUTIVE SUMMARY

The purpose of this Thought Paper is to explore the benefits of replacing proprietary communication protocols with industry standard protocols as a vehicle to increase the velocity, efficiency, and effectiveness of mortgage information processing.

This paper was written by The *Data Formats and Transmission Management Alignment Group* of the *Expanding Integration and Distribution Capabilities Team*. The team focused on analyzing and comparing web services communication protocols currently used in the industry. The team also conducted an industry survey on the current state of data communication methodology.

Research focused primarily on the publically-available protocols such as SOAP and REST (used respectively by the 92% and 77% of respondents of the survey); however, it also included the proprietary Fannie Mae XIS protocol (reportedly used by the 58% of the survey respondents.)

This paper includes analysis of the various aspects of the communication protocols, in particular the integration components such as User and Message Security and Quality of Service in both two-party and multi-party integration. Other considerations such as data formats, payload efficiency, caching, support of multiple representation of data, use of the synchronous and asynchronous services, and formal service specifications are also analyzed.

The study results led the authors to conclude that given the current state of technology, SOAP web services communication protocol enforced by the WS-\* specifications offers the most effective methodology to enhance business-to-business (B2B) mortgage information processing.

## 2 OVERVIEW

### 2.1 Introduction

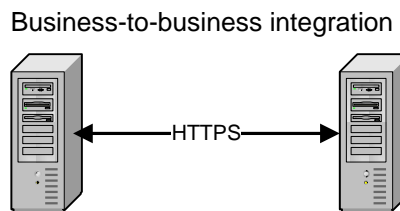
Technology participants in the mortgage industry integrate their B2B applications using a mix of protocols and standards. To be successful, each business-to-business integration has to overcome common integration challenges; however, when an implementation is based on non-standard protocols, implementation costs and time-to-market are likely to increase significantly.

### 2.2 Objective and Scope

The high-level objective of this paper is to evaluate existing web services messaging protocols and recommend a direction for current and future industry use cases. In particular, this paper focuses on the benefits of using SOAP versus REST, as these are the most widely used industry-standard integration web services, and how these web service messaging protocols can support business objectives.

- SOAP stands for Simple Object Access Protocol, a specification for exchanging structured information that relies on XML.
- REST stands for Representational State Transfer, a style of software architecture for distributed systems

This paper examines B2B, business-to-business integration, not B2C, business-to-consumer integration. B2B is typically implemented by making a web service call over an HTTP transport service. For purposes of this paper, the focus is on two-way, point-to-point integrations between XIS, SOAP, and/or REST connections.



This paper does not discuss validation, governance, or best practices of the web service messaging protocol as that topic is covered in the *Thought Paper: Expanding Integration & Distribution Capabilities*. Likewise, development of Data Formats and Data Definition standards are covered in *Thought Paper: Portability Standards for Documents & Data*.

## 2.3 Survey

To determine how web service messaging protocols are being used in the mortgage industry, we developed a survey in collaboration with the Fannie Mae Innovation Challenge Program. The survey was distributed to a broad spectrum of CIOs in the mortgage industry as well as Innovation Challenge participants. The survey responses are reviewed in this document and provide insights into the current state of the industry as well as information about future needs.

Detailed responses can be found in Appendix B.

## 2.4 Survey Response Categories

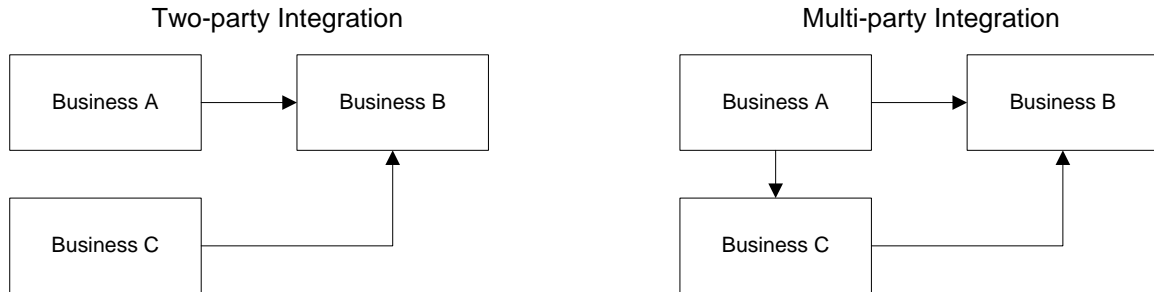
Twenty-six (26) anonymous participants responded to this survey. There were three categories of questions:

Environment	Integration Components*	Other Considerations
100% Operate in B2B environments	77% Operate in a single security domain	65% Do not need caching as it relates to HTTP GET versus HTTP Post requests.
46% Operate in B2C environments	46% Use Federated Identity Management across multiple security domains	62% Agree that it would be extremely valuable for the mortgage industry to leverage a common integration protocol.
62% Rate their experience with XIS as time consuming and require special skills	92% That pass information between more than two systems, think that message security is important	58% Need 9 - 12 months to make a transition from their current communication protocol to another communication protocol
92% Use SOAP		
77% Use REST	73% Have Quality-of-Service requirements such as reliable messaging and transactional integrity	
62% Use XIS		
73% Pass information between more than two systems		

\* Integration Components are common aspects of integration regarding User Security, Message Security, and Quality of Service. The complexity of the Integration Components will vary greatly, depending on the level of integration.

## 2.5 Level of Integration

In general, there are two types of B2B integration: two-party integration and multi-party integration.



Two-party integration is a typical B2B integration where the integration is between two parties and there is a single security domain. In the first diagram above, Business A integrates with Business B. Business C also integrates with Business B, and it is two-party integration in each case.

Multi-party integration describes B2B integration where the integration is between more than two parties and there are multiple security domains. In the second diagram above, Business A integrates with Business B as well as Business C. Business B and Business C will have separate security domains.

A characterization of two-party integration and multi-party integration follows:

Two-party Integration	Multi-party Integration
<ul style="list-style-type: none"> <li>• Single central security authority or multiple security domains without trust</li> </ul>	<ul style="list-style-type: none"> <li>• Decentralized security with multiple independent security authorities with established trust</li> </ul>
<ul style="list-style-type: none"> <li>• Simple point-to-point message exchange patterns</li> </ul>	<ul style="list-style-type: none"> <li>• More end-to-end message exchange patterns where the message may pass through an intermediary</li> </ul>
<ul style="list-style-type: none"> <li>• Probably represents a large percentage of current integration patterns.</li> </ul>	<ul style="list-style-type: none"> <li>• May represent a smaller number of integration patterns, but it would be expected to grow in the future as business develop partnerships to provided additional services for their customers</li> </ul>

The analysis of the integration components includes both points of view: two-party integration and multi-party integration. This section is organized to compare the differences between two-party integration and multi-party integration including: User Security, Message Security, and Quality of Service.

### 3 ANALYSIS AND SCORING

#### 3.1 Scoring

Each category covers a particular integration consideration and is scored to indicate whether SOAP or REST provides an improvement over XIS. The following table illustrates the possible permutations:

<ul style="list-style-type: none"><li>Neither SOAP nor REST offer an advantage over XIS, the score card will be without color.</li></ul>	SCORE SOAP WS-* REST
<ul style="list-style-type: none"><li>When SOAP provides an advantage over XIS and REST, the score card will be blue.</li></ul>	SCORE SOAP WS-* REST
<ul style="list-style-type: none"><li>If REST provides an advantage over XIS and SOAP, the score card will be green.</li></ul>	SCORE SOAP WS-* REST
<ul style="list-style-type: none"><li>If both SOAP and REST provide an advantage over XIS, the score card will be blue and green.</li></ul>	SCORE SOAP WS-* REST

Note: SOAP WS-\* stands for the combination of SOAP and the body of web service specifications known as WS-\*. A high-level view is provided in Appendix C.

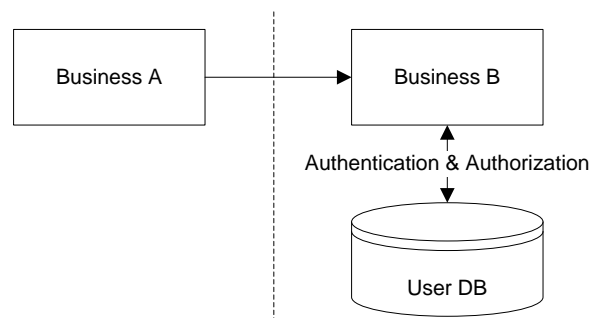
#### 3.2 Integration Components Analysis

##### 3.2.1 User Security (Authentication and Authorization)

User security has two parts, authentication and authorization. We will take a look at them in the context of two-party integration and then multi-party integration.

##### 3.2.1.1 Two-party User Security

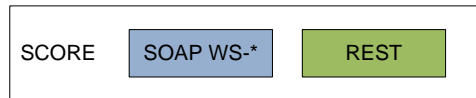
In a two-party integration scenario, there is typically a single authority in control of identity management as well as role assignment and authorization.





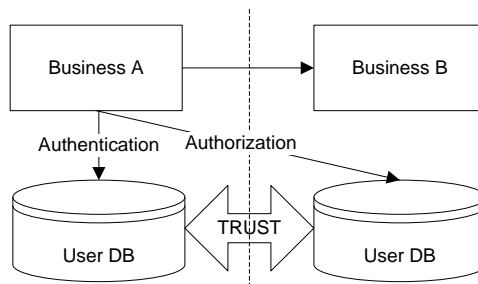
Authentication techniques can be used over HTTP and used with a protocol such as WS-Security, or even be implemented with a proprietary protocol. In this environment, both SOAP and REST support a wider range of authentication options than XIS.

**Two-Party User Security SCORE: SOAP and REST are both better than XIS**



**3.2.1.2 Multi-party User Security**

In a multi-party user security scenario, the responsibilities of authentication and authorization are commonly divided using a claims-based based approach.

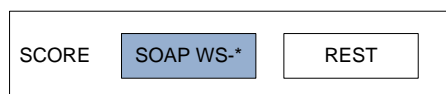


The Security Assertion Markup Language, SAML, is used to communicate claims of authenticity and authorization. One respondent in our survey identified SAML as a requirement for their identity management needs.

The process of setting up trust between two businesses and the process to create security tokens is out of scope of this paper.

SOAP has specifications to support SAML as well as other security tokens such as an X.509 certificate and Kerberos ticket. Having specifications with WS-Security and WS-Federation gives SOAP an advantage for multi-party integration.

**Multi-Party SCORE: SOAP is better than XIS**

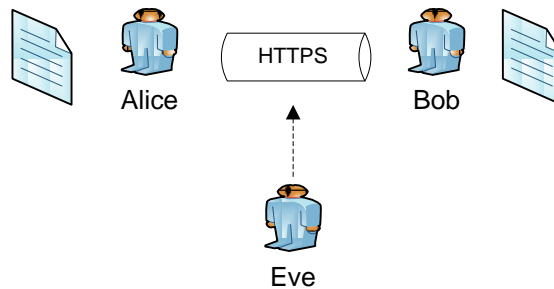


### 3.2.2 Message Security (Integrity and Confidentiality)

Message security has two parts: integrity and confidentiality. Integrity is the concern that the message has not been tampered with and confidentiality means that the message cannot be viewed by any unintended observers.

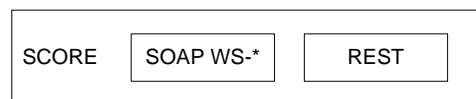
#### 3.2.2.1 Two-party Message Security

In two-party integration, using HTTPS provides protection from message tampering while it is in transit as well as confidentiality.



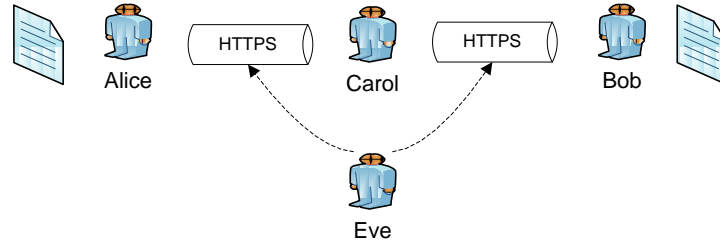
In this diagram, Alice can transmit her document to Bob securely. Eve, the eavesdropper cannot eavesdrop on the transmission. As HTTPS can be used by both SOAP and REST, the result is a tie.

**Two-party Message Security SCORE: Neither SOAP nor REST provide an advantage over XIS**



### 3.2.2.2 Multi-party Message Security

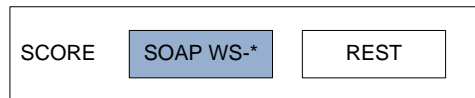
In a multi-party integration, HTTPS can provide protection from eavesdropping while the message is in transit, but it cannot protect against tampering from a middle man.



In this scenario, Alice is transmitting a message and Bob is the intended receiver. However, due to business workflows, the document passes through one or more middle men. The use of digital signatures can be used to protect against tampering. Encryption could be used to protect sensitive information so that only the intended recipient could decode the message.

SOAP has the WS-Security specification to augment the protection provided by HTTPS.

**Multi-party Message Security SCORE: SOAP is better than XIS**



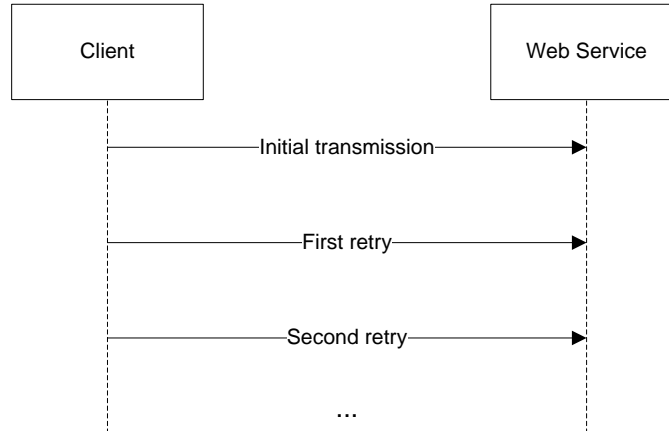
### 3.2.3 Quality of Service (Reliability and Transactions)

A communication channel can have several levels of quality. Two of the most common areas of concern are reliability and transactions.

#### 3.2.3.1 Two-Party Quality of Service - Two-party Reliability

Even though we have guaranteed transmission of the messages over TCP/IP and HTTP, that doesn't guarantee that the message can be processed and a response is received by the caller. Therefore, in a Two-party integration scenario, retry algorithms are commonly built into each custom integration.

### Transmission retries for reliability



That is, if the caller receives an error, or doesn't receive a proper response within a certain period of time, it will try again later. The amount of time to wait and the number of times to retry are specific to each application and have to be agreed upon with each participant.

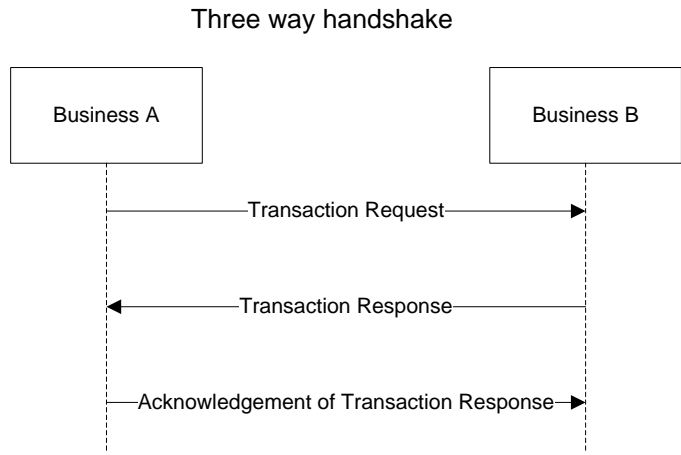
The use of transmission retries is a design issue that is independent of the communication protocol. In other words, retries can be implemented equally well by XIS, SOAP, or REST systems.

If the preference is to use a standard way of establishing reliable messaging with integration partners, SOAP has a specification, WS-Reliable Messaging that can be used as a building block to build a complete messaging solution.

#### 3.2.3.2 Two-party Transactions

Transactions may be required in specialized business situations. The transfer should either succeed and the item ends up with the recipient, or the transfer should fail, and the item should still be with the sender. A common way to manage a transaction between two parties is to use a three-way handshake. It requires three messages:

1. The request to start a transaction
2. The response of the result of the transaction
3. An acknowledgement of the response



The communication to perform a three-way handshake can be done with any of the communications protocols, XIS, SOAP, or REST.

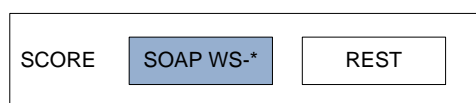
REST is stateless and by definition, cannot hold a transaction. It therefore will have a challenge to support transactions in a standardized manner. However, with REST, a separate resource may be needed to act as a lock.

If handling transactions in a standard manner is preferred, SOAP has a specification, WS-AtomicTransaction.

### 3.2.3.3 Two-party Quality of Service Score

Two-party integration practices may include the use of retries to achieve reliability and a three-way handshakes to achieve transactional agreement. It is assumed that one or both of these techniques are in wide use in integrating systems in the mortgage industry. While it is certainly possible to continue the practice of developing one-off solutions in two-party integrations, the use of standards such as WS-ReliableMessaging and WS-AtomicTransaction specifications with SOAP may be an aid to reduce integration costs and time to market.

#### Two-Party Quality of Service SCORE: SOAP is better than XIS

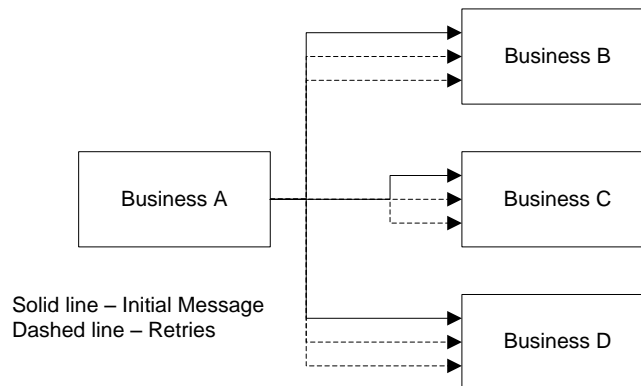


### 3.2.4 Multi-Party Quality of Service

We will look at multi-party reliability and multi-party transactions before scoring multi-party quality of service.

#### 3.2.4.1 Multi-party Reliability

For Multi-party integration, with each new integration custom implementations that maintain reliability can become expensive. Suppose Business A implements a retry practice with each of the businesses with which it integrates.



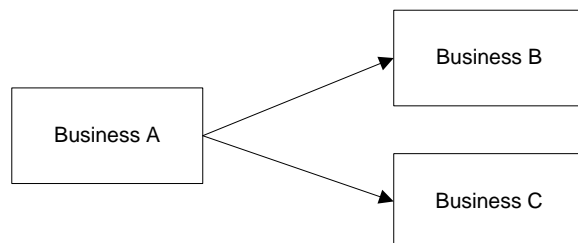
If Business A had many integration partners, it would have to keep track of all the retries with each integration partner. For scalability, it may be easier to use SOAP as the communication protocol and leverage the WS-ReliableMessaging specification to manage reliability in a common manner.

REST, on the other hand, does not have a standard for reliable messages. This does not mean that REST is unreliable; it just means that the integration needs a proprietary retry strategy to achieve reliability with each business.

#### 3.2.4.2 Multi-party Transactions

In a multi-party scenario, transactions become more complicated. Assume there is a requirement for a transaction to happen between A and B, as well as A to C. These transactions need to be coordinated and both must succeed or they both fail.

### Multi-party Transaction

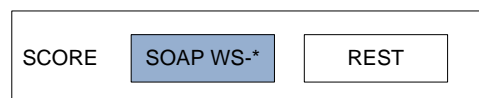


With SOAP, it is possible to coordinate a set of transactions with multiple parties. In this case, SOAP would not only have to use the WS-AtomicTransaction specification, but it would also need to use WS-Coordination. The WS-\* specifications are designed to be mixed and matched when needed.

#### 3.2.4.3 Multi-party Quality of Service Score

SOAP has WS-ReliableMessaging, WS-AtomicTransaction, and WS-Coordination protocols to leverage specifications to meet complex multi-party integration needs.

**Multi-party Quality of Service SCORE: SOAP is better than XIS**

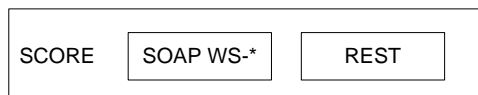


### 3.3 Other Considerations Analysis

#### 3.3.1 Data Formats and Data Definitions

A critical component of integration is to have a common definition of formats and terms. An example would be MISMO 2.6 GSE.

**Data Formants and Data Definitions SCORE: Since XIS, SOAP and REST support XML (and XSDs), they should be even.**



### 3.3.2 Payload Efficiency

A common concern in IT is the efficiency of the system. In this context, we are referring to the payload in the HTTP body. In the samples below, the common payload is highlighted in yellow and the overhead in SOAP is highlighted in blue.

#### *REST Response Sample:*

```
<?xml version="1.0" encoding="utf-8" ?>
<response>
  <m:StockPrice xmlns:m="http://www.example.org/stock">
    <m:StockName>IBM</m:StockName>
  </m:StockPrice>
</response >
```

#### **SOAP Response Sample:**

```
<?xml version="1.0" ?>
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope"
  xmlns:s="http://tempuri.org/service">
  <env:Body>
    <m:GetStockPrice xmlns:m="http://www.example.org/stock">
      <m:StockName>IBM</m:StockName>
    </m:GetStockPrice>
  </env:Body>
</env:Envelope>
```

Simply put, REST requires fewer characters to provide a response than SOAP, which includes the overhead of the SOAP header and body.

#### **Payload Efficiency SCORE: REST is better than XIS**

SCORE	SOAP WS-*	REST
-------	-----------	------

### 3.3.3 Caching

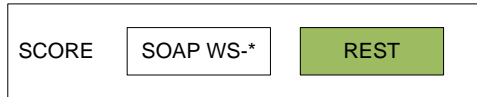
Caching can impact performance and scalability. SOAP uses an HTTP POST to transmit data. That means the HTTP POST is used when sending data as well as when retrieving data. REST uses an HTTP POST to send data, but it can use an HTTP GET to retrieve data.



When the data being retrieved is the same for many clients, caching the result can really help with performance.

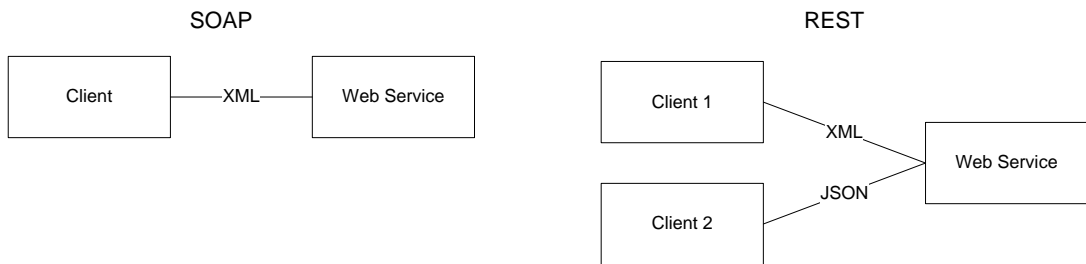
Caching will have a less significant benefit if there are only a couple of clients and the data isn't retrieved often or the data changes frequently.

**Caching SCORE: REST is better than XIS**



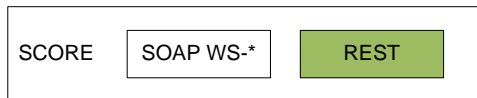
**3.3.4 Multiple Representations of Data**

SOAP presumes an encoding standard of the data as XML while REST allows clients to request information in a specific format (i.e., XML or JSON).



The requirement of multiple representations will depend on your business requirements where JSON is more likely to be needed in B2C (web browser) scenarios.

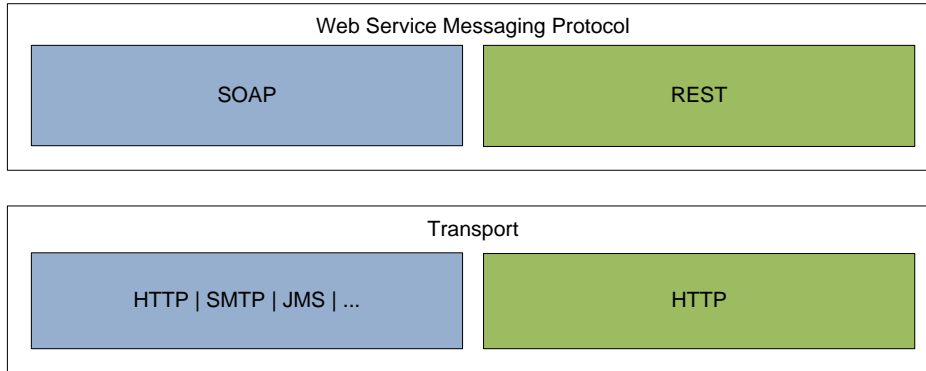
**Multiple Representations of Data SCORE: REST is better than XIS**



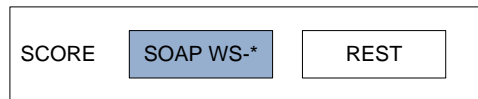
**3.3.5 Message Transport Options**

Up to this point, all message or data transfer methods use HTTP. But, what if we have a heterogeneous environment and require support from another transport protocol such as JMS or SMTP?

If an enterprise needs to integrate with a system that used a transport protocol other than HTTP, only SOAP provides the capability. The following is a simplified architectural diagram that shows how the Messaging layer is over the Transport layer.



**Message Transport Options SCORE: SOAP is transport agnostic and can be used over different transfer protocols. REST only works over HTTP.**



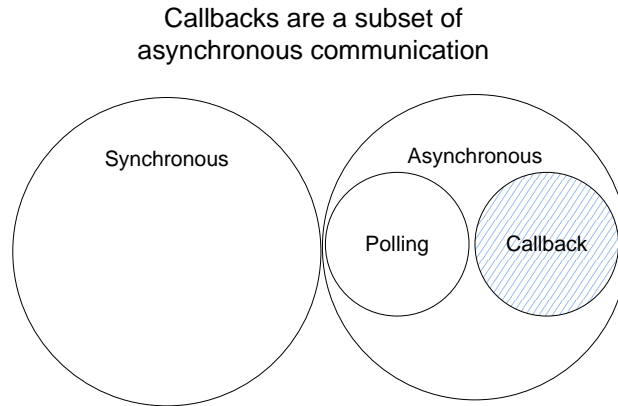
### 3.3.6 Synchronous and Asynchronous Services

All communication protocols, XIS, SOAP, and REST can be used to make both synchronous and asynchronous calls. If an asynchronous call is used, there are two ways for the response to be returned: 1) polling by the client or 2) the server can call a callback.

If the polling method is used, any of the communication protocols, XIS, SOAP, and REST can be used equally well.

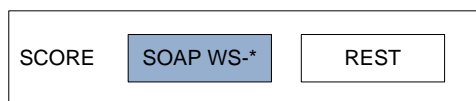
In fact, XIS uses an interesting hybrid of synchronous and asynchronous calls which requires any client to program for both types of communication. This hybrid approach allows for synchronous calls to be used initially which allows for optimal response times for the majority of transactions as responses are typically returned in a few seconds. The asynchronous process is built as a safety net to ensure calls are not kept open for an extended amount of time. A time out is set to trigger an asynchronous response rather than keeping the synchronous call open until a response is returned.

If the callback method is to be used, the challenge is to use a standard element in the request to specify the callback address. The following Venn diagram illustrates the subset of cases where callbacks are used in communication.



If REST was used, the callback address would have to be passed in somewhere in the request at a place to be specified by the service provider. It could vary from provider to provider. SOAP, on the other hand, has a specification called WS-Addressing to pass around a callback address. Therefore, if multiple businesses in the mortgage industry followed the same specification, the effort required for integration may be reduced.

### **Synchronous and Asynchronous Services SCORE: SOAP is better than XIS**



### **3.3.7 Formal Service Specifications**

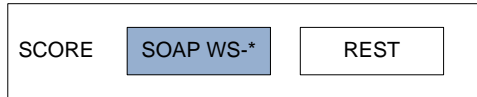
A consumer of a web service requires information on how to use the service. Having a formal specification that describes the valid input parameters or output responses goes a long way when integrating B2B.

SOAP uses WSDL, the Web Service Definition Language to provide a formal description of the messages that can be accepted by the web service. It is currently at version 2.0 and was recommended by the W3C in June 2007..

REST can use WADL, Web Application Description Language to describe the set of resources available through the web service. WADL was submitted to the World Wide

Consortium in August 2009, but there are no current plans to standardize it and it is not widely supported.

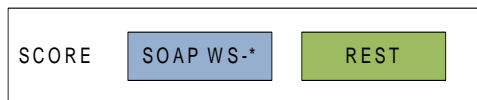
**Formal Service Specifications SCORE: SOAP is better than XIS**



**3.3.8 Industry Standard Tools and Support**

One of the issues with XIS is that it is not an industry standard. That means that there is a learning curve that can affect the development and deployment of an integration. SOAP and REST are familiar and popular according to our survey.

**Industry Standard Tools and Support SCORE: SOAP and REST are better than XIS**



## 4 ANALYSIS SUMMARY

The scores include analysis of the two-party integration scenario as well as the multi-party integration scenario. Other considerations are evaluated separately as they varies vary according to different business needs.

Criteria	SOAP	REST
<b>Two-Party Integration</b>		
User Security (Authentication and Authorization)	1	1
Message Security (Integrity and Confidentiality)	0	0
Quality of Service (Reliability and Transactions)	1	0
<b>Two-Party Sub-Score</b>	<b>2</b>	<b>1</b>
<b>Multi-Party Integration</b>		
User Security (Authentication and Authorization)	1	0
Message Security (Integrity and Confidentiality)	1	0
Quality of Service (Reliability and Transactions)	1	0
<b>Multi-Party Sub-Score</b>	<b>3</b>	<b>0</b>
<b>Other Considerations*</b>		
Data Formats and Data Definitions	0	0
Payload Efficiency	0	1
Caching	0	1
Multiple Representations of Data	0	1
Message Transport Options	1	0
Asynchronous and Synchronous Services	1	0
Formal Service Specifications	1	0
Industry Standard Tools and Support	1	1
<b>Other Considerations Sub-Score</b>	<b>4</b>	<b>4</b>
<b>Un-weighted Total</b>	<b>7</b>	<b>5</b>

\* These “other considerations” may not apply to every integration scenario and are likely to have a lower weight in importance when compared to the Integration Components. For example, if a firm has a two-party integration where performance and scalability are the highest priorities, then REST may be a better fit. On the other hand, if the integration needs to use alternate message transport protocols, then SOAP may be a better fit.

## 5 RECOMMENDATIONS

REST is very popular and may be the best strategy for certain two-part integration scenarios; however, SOAP better addresses the future needs of the mortgage industry. Considerations for favoring SOAP include:

- Many organizations are already familiar with SOAP. It is currently used by 92% of the survey respondents.
- It offers stronger data contact for B2B integration with WSDL and XSD specifications.
- It supports advanced, multi-party integrations for user security, message security, and quality of service.

In the end, using a particular communications protocol has to make business sense. At the present time, SOAP has the more mature set of specifications, but that doesn't mean we can take our eyes off industry trends as new standards may emerge.

### 5.1 *Current SOAP Integrations*

Businesses that are currently using SOAP can add additional advanced integration features as needed:


User Security (Authentication and Authorization)	Message Security (Integrity and Confidentiality)	Quality of Service (Reliability and Transactions)
SOAP		

For example, businesses can start off with their current use of SOAP and as the business need for federated security grows, the standard can be adopted by integration participants. Meanwhile, if improvements in message integrity and confidentiality are needed, adoption of those standards can proceed in an independent manner.

SOAP can therefore meet the current needs of B2B integration as well as future needs as characterized by the two-party and the multi-party integration models.

### 5.2 *New SOAP Integrations*

For new B2B integration projects, the recommendation is to use SOAP, assuming all business requirements are satisfied. Using SOAP for new integrations provides the foundation for future



extensions if the needs of the business grow to include multi-party user security, message security, or quality of service.

## **6 STRATEGY FOR LEGACY INTEGRATIONS**

We do not recommend switching any existing non-SOAP integration to SOAP just to switch to SOAP. Retooling a web service is very expensive and not only affects the service provider, but also all of the clients. Any existing integration provides business value and it will be up to each business to evaluate if the expense of switching communication protocols will provide a reasonable return on investment. If wholesale change is cost prohibitive, but some of features of multi-party integration components are desired, we suggest using a protocol gateway to act as an intermediary. Using a protocol gateway can lower the cost of integrating a legacy system with multi-party integration components. The applicability of the protocol gateway will depend on the details of the environment and will be left for each business to evaluate.

## **7 NEXT STEPS**

The survey was conducted over a small sample set and our survey results represent a fraction of the integration needs in the mortgage industry. We should expand the survey to cover a broader cross section of the secondary market participants.

The communications protocol is just one part of a larger and complex system. It has many touch points with integration components such as user security, message security, and quality of service. Each of these areas should be explored more fully to get a better understanding to the needs and best practices in the mortgage industry.

The different phases of the mortgage lifecycle have different communications protocol requirements and more research may be required to understand the message exchange patterns and integration components involved.

## 8 APPENDIX

### 8.1 Appendix A – Glossary of Terms

Term	Definition
<b>Asynchronous Web Service</b>	A web service call that returns quickly, but the final response would need to be picked up by polling or by a callback call.
<b>Authentication</b>	The act of confirming the identity of the person or software program.
<b>Authorization</b>	The function of specifying access rights to resources.
<b>B2B</b>	Business to Business
<b>B2C</b>	Business to Consumer
<b>Digital Signature</b>	A scheme for demonstrating the authenticity of a digital message or document.
<b>Federated Identity Management</b>	Federated Identity Management falls under the umbrella of Identity Management and amounts to having a common set of policies, practices, and protocols to manage identities and trust across organizations.
<b>HTTP</b>	Hypertext Transfer Protocol
<b>HTTP GET</b>	A method to retrieve data via HTTP
<b>HTTP Post</b>	A method to submit data via HTTP
<b>HTTPS</b>	Hypertext Transfer Protocol Secure
<b>Identity Management</b>	The management of individual identities of people or things (such as a service), their authentication and authorization within or across system boundaries.
<b>JMS</b>	Java Message Service - A Java Message Oriented Middleware API for sending messages between two or more clients.
<b>JSON</b>	JavaScript Object Notation is a text-based open standard for human-readable data interchange. It is primarily used to transmit data between a server and a web application.
<b>Legacy System</b>	A system that is installed and working, but it may not be up to current standards or protocols. It doesn't necessarily mean that the system is obsolete.
<b>Multi-party integration</b>	Multi-party integration is used to describe B2B integration where the integration is between more than two parties and there are multiple security domains
<b>QoS</b>	Quality of Service - In the context of a service oriented architecture, quality of service refers to aspects of the communication such as reliability and transactions.
<b>REST</b>	Representational state transfer - a style of software architecture for distributed systems.
<b>SAML</b>	Security Assertion Markup Language - an open standard data format for exchanging authentication and authorization data between parties.
<b>Security Domain</b>	Is a collection of computers, networks, or applications that fall under a specific security protocol for authentication and quite often authorization.
<b>SOAP</b>	Simple Object Access Protocol - a specification for exchanging structured information that relies on XML.





Term	Definition
<b>Synchronous Web Service</b>	A web service call that blocks until the response is returned.
<b>Transport Protocol</b>	A communications protocol responsible for establishing a connection and ensuring that all data has arrived safely.
<b>Two-party integration</b>	The process of bringing data or a function from one application program together with that of another application program.
<b>Ultra Messaging</b>	A family of messaging middleware products from Informatica
<b>W3C</b>	The World Wide Web Consortium is the main international standards organization for the World Wide Web.
<b>WADL</b>	Web Application Description Language
<b>Web Service</b>	A method of machine-to-machine interaction over a network.
<b>WS-*</b>	A collection of Web Service Specification such as WS-Security, WS-Federation, and WS-Atomic Transaction which cover a variety of topics such as messaging, metadata exchange, security, reliable messaging, and transactions.
<b>WSDL</b>	Web Service Definition Language
<b>XIS</b>	XML Integration Services, Fannie Mae's proprietary protocol
<b>XSD</b>	XML Schema Definition - a formal specification to describe elements in an XML document.

## 8.2 Appendix B – Detailed Survey Results

These questions are to get an understanding of environments that participants in the mortgage industry are involved with.

- 1) **What communications protocols are you currently using in your business?**  
(Respondents allowed to choose **multiple** responses)

Response	Chart	Frequency	Count
XIS		61.5%	16
<b>SOAP</b>		<b>92.3%</b>	<b>24</b>
REST		76.9%	20
Other (Specify):		19.2%	5
		<b>Valid Responses</b>	<b>26</b>
		<b>Total Responses</b>	<b>26</b>

- 1b) **What other communications protocols are you currently using in your business?**

Response	Frequency	Count
WSDL		
UltraMessaging		
JSON		
FTP, HTTP Post, SMTP		
		<b>Valid Responses</b>
		<b>4</b>
		<b>Total Responses</b>
		<b>26</b>

2) **How would you rate your experience with XIS integration with Fannie Mae today?**  
 (Respondents may only choose a **single** response)

Response	Chart	Frequency	Count
Simple to integrate		34.6%	9
Time consuming and requires specialized skills		<b>61.5%</b>	<b>16</b>
Difficult		3.8%	1
		<b>Valid Responses</b>	<b>26</b>
		<b>Total Responses</b>	<b>26</b>

3) (Optional) **Comments regarding problems:**

Response		
I don't currently use it.		
The experience with XIS integration is simple, yet it requires a level of knowledge about industry standards and requires a level of specialized skills.		
XIS is significantly more time consuming to setup and offers no benefits over a more standardized SOAP platform.		
Don't use it		
We do not use XIS.		
Currently do not work with XIS Integration. Required field for 2.a N/A was not a choice.		
We have had no experience with XIS		
Technically, having to integrate using a multi part form parameters was not ideal. Also, having to code to handle delayed processing was problematic. Business Requirements, too much time was spent clarifying mappings.		
		<b>Valid Responses</b>
		<b>8</b>
		<b>Total Responses</b>
		<b>26</b>

4) **What business environment does your firm operate in?**  
 (Respondents may only choose a **single** response)

Response	Chart	Frequency	Count
Business to business (B2B)		53.8%	14
Business to consumer (B2C)		0.0%	0
Both		46.2%	12
		<b>Valid Responses</b>	<b>26</b>
		<b>Total Responses</b>	<b>26</b>

5) **How many systems does your information pass between?**  
 (Respondents may only choose a **single** response)

Response	Chart	Frequency	Count
Two systems		26.9%	7
More than two systems (please answer question 10b)		73.1%	19
		<b>Valid Responses</b>	<b>26</b>
		<b>Total Responses</b>	<b>26</b>

6) **What are your Identity Management needs? (Check all that apply)**  
 (Respondents may choose **multiple** responses)



Response	Chart	Frequency	Count
Authentication & Authorization in a single security domain		76.9%	20
Federated Identity Management across several autonomous security domains		46.2%	12
Other (Specify):		7.7%	2
		<b>Valid Responses</b>	<b>26</b>
		<b>Total Responses</b>	<b>26</b>

6b) **Optional – Specify Other**

Response	Frequency	Count
SAML claims-based authentication and authorization		
Multiple security domains without federated trust		
		<b>Valid Responses</b>
		<b>2</b>
		<b>Total Responses</b>
		<b>26</b>

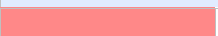

7) **If the information is being passed between more than two systems, is it important to protect information from unauthorized tampering or eavesdropping?**

(Respondents may only choose a **single** response)

Response	Chart	Frequency	Count
Yes		91.7%	22
No		8.3%	2
Not Answered			2
		<b>Valid Responses</b>	<b>24</b>
		<b>Total Responses</b>	<b>26</b>

8) **Do your transactions have Quality of Service (QoS) requirements? For example, do you need Reliable Messaging or Transactional Integrity?**

(Respondents may only choose a **single** response)



Response	Chart	Frequency	Count
Yes (please answer question 8b)		73.1%	19
No (please go to question 9)		26.9%	7
		<b>Valid Responses</b>	<b>26</b>
		<b>Total Responses</b>	<b>26</b>

8 b) **If yes, please specify your critical QoS concerns:**

Response
1. Reliable messaging is critical for message acknowledgement and delivery status awareness for sender and receiver applications and web services.
2. Need to know that a transmission was completed and was valid.
3. Data Integrity, Security
4. Processing time
5. Service cannot go down
6. Schema validation; error handling
7. Guaranteed messaging. Do not require transactions
8. Be sure all transactions are successfully completed and rollback any data transaction in case of failure
9. reliable messages, transaction integrity
10. As a financial services provider, Quality of Service is a high priority in all of the services we provide.
11. Transaction Integrity, throughput time
12. We have to have a Reliable Transaction between interfaces with error handling and notification of system availability
13. We require confirmation of delivery beyond a traditional hand-shake.
14. When we integrate systems it is very important to ensure that messages are processed reliably when requested It's expensive to create to create technical or business process controls to ensure things happened or perform retry.
15. Insure complete transaction response
16. Auditable, Reliable, & Secure
17. All our work has contractual service agreements.





9) **Does your application need caching as it relates to HTTP GET vs HTTP POST?**

(Respondents may only choose a **single** response)

Response	Chart	Frequency	Count
Yes (please answer question 9b)		34.6%	9
No (please go to question 10)		<b>65.4%</b>	<b>17</b>
		<b>Valid Responses</b>	<b>26</b>
		<b>Total Responses</b>	<b>26</b>




9b) **If yes, how critical is caching to your application?**

(Respondents may only choose a **single** response)

Response	Chart	Frequency	Count
Very critical		7.7%	1
Critical		53.8%	7
Nice to have		15.4%	2
Not important		23.1%	3
Not Answered			13
		<b>Valid Responses</b>	<b>13</b>
		<b>Total Responses</b>	<b>26</b>




10) **How do you value the need for the mortgage industry to leverage a common integration protocol to exchange data with the GSEs and with each other?**

(Respondents may only choose a **single** response)

Response	Chart	Frequency	Count
<b>Extremely valuable</b>		<b>61.5%</b>	<b>16</b>
Valuable		30.8%	8
Somewhat		7.7%	2
Not important		0.0%	0
		<b>Valid Responses</b>	<b>26</b>
		<b>Total Responses</b>	<b>26</b>

11) **If your firm changed from one protocol to another (e.g. XIS to one of the industry standards such as SOAP or REST) what would be the impact in terms of time to adapt?**

(Respondents may only choose a **single** response)

Response	Chart	Frequency	Count
Low impact (3 - 6 months)		34.6%	9
<b>Medium impact (9 - 12 months)</b>		<b>57.7%</b>	<b>15</b>
High impact (well over 18 months)		7.7%	2
		<b>Valid Responses</b>	<b>26</b>
		<b>Total Responses</b>	<b>26</b>

### 8.3 Appendix C – Web Service Architecture Comparison

The following diagram is a comparison of web service architecture between SOAP and REST and is provided to help provide context for the protocols and specifications that are mentioned in this paper.

