Quality Model for Web Services

September 2005

Document identifier:

WSQM -2.0

Location:

Editor:

Eunju Kim (NCA), Youngkon Lee (KOREA Polytechnic University)

Abstract:

The purpose of this document is to provide a model for Web services quality management and quality factors in the process of developing and using Web services. We define the consistent and systematic conceptual model of Web services quality, which may be used by intimate associates, i.e. stakeholders, developers, service providers, and customers of Web services.

Status:

This document is a Working Draft.

Table of Contents

1 Introduction....5
1.1 Purpose....5
1.2 Compliance....5
2 References and Acronyms....6
2.1 Normative References....6
2.2 Acronyms 7
3 Web Services Quality Model....8
3.1 Quality Factor of Web Services....9
3.1.1 Web Services Quality as a Service....9
3.1.2 Quality Service Model....9
3.2 Quality Associates for Web Services....10
3.2.1 Stakeholder and Developer....11
3.2.2 Developer....11
3.2.3 Provider 11
3.2.4 Consumer....11
3.2.5 QoS Broker 11
3.2.6 Quality Assurer 12
3.2.7 Quality Manager 12
3.3 Quality Activity of Web Services....12
3.3.1 Development Quality Contract 14
3.3.2 Web Services Quality Contract 14
3.3.3 Management Quality Contract....15
4 Business Value Quality....16
4.1 Definition....16
4.1.1 Type....16
4.2 Quality Sub-factors....16
4.2.1 Business Suitability....17
4.2.2 Business Effect....17
4.2.3 Business Recognition Level....18
4.3 Quality Contracts 18
4.4 Quality Associates 19
4.5 Related Standard 19
5 Service Level Measurement Quality....20
5.1 Definition....20

5.1.1 Type....20
5.2 Quality Sub-factors....20
5.2.1 Performance....20
5.2.2 Stability 21
5.3 Quality Contracts 22
5.4 Quality Associates 22
5.5 Related Standards 23
6 Interoperability Quality....24
6.1 Definition....24
6.1.1 Type....24
6.1.2 Quality Sub-factors....24
6.2 Quality Sub-factors....24
6.3 Quality Contracts....24
6.4 Quality Associates....25
6.5 Related Standards 25
7 Business Processing Quality 27
7.1 Definition 27
7.1.1 Type....27
7.2 Quality Sub-factors....27
7.2.1 Reliable Messaging....28
7.2.2 Message Context....28
7.2.3 Transaction....28
7.3 Quality Contracts 29
7.4 Quality Associates 29
7.5 Related Standards 30
8 Manageability Quality 32
8.1 Definition 32
8.1.1 Management Functions 32
8.1.2 Manageable Services 32
8.1.3 Management Level 32
8.2 Quality Sub-factors....33
8.2.1 Manageable Level....33
8.2.2 Managed Levels 33
8.3 Quality Contracts 34
8.4 Quality Associates 34
8.5 Related Standard 35
9 Security Quality....36

9.1 Definition 36

9.1.1 Qualities of Security Services..36

9.1.2 Security Service Level..37

9.2 Quality Sub-factors 38

9.2.1 Sub-factor DefinitionsTransport Level..38

9.2.2 Message Level 39

9.2.3 Security Factors & Related Technology Mapping 40

9.2.4 Security Profile 41

9.3 Quality Contracts 43

9.4 Quality Associates 44

9.5 Related Standards 45

1 Introduction

System integration through Web Services gains in more importance as the focus of the Internet business model is moving from B2C to EAI, B2B. The successful system integration through Web Services means providing faster and more reliable services as if remote Web Services are local Web Services. In other words, high quality of Web Services is being recognized as the critical element of successful business based on SOA (Service Oriented Architecture) This document presents Web Services Quality Model so that associates may precisely understand and describe Web Services quality.

1.1 Purpose

This document is to present Web Services Quality Model which MUST be considered while performing all the necessary interactions such as order, development, management and maintenance among the associates during lifecycle of Web Services. The model is classified into 3 sub-models: Quality Associates Model, Quality Contract Model, and Quality Management Model.

1.2 Compliance

This document suggests Web Services Quality Model (WSQM) in conceptual level. Therefore, in order to apply this model onto real world, the quality properties and the scope sub-factors must be defined according to the characteristics of Web Services. Meanwhile, due to its concept-limited description, it is required to create the quality check list corresponding with the framework of WSQM in this document.

2 References and Acronyms

2.1 Normative References

- ISO 9126
  URL: http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39752

- WS-I Basic Profile 1.1 ▪
  URL: http://www.ws-i.org/Profiles/BasicProfile-1.1-2004-08-24.html

- WS-I Basic Security Profile Version 1.0
  URL: http://www.ws-i.org/Profiles/BasicSecurityProfile-1.0-2004-05-12.html

- WS-I Simple SOAP Binding Profile Version 1.0 ▪
  URL: http://www.ws-i.org/Profiles/SimpleSoapBindingProfile-1.0-2004-08-24.html

- OASIS WS-Reliable Messaging

  URL: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsrm

- OASIS BPEL4WS(Business Process Execution Language For Web service)

  URL: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsbpel

- OASIS WS-CAF(Composite Application Framework)

  URL: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ws-caf

- W3C WS-CDL (Web service Choreography Description Language)
  URL: http://www.w3.org/TR/2004/WD-ws-cdl-10-20040427/

- OASIS WSDM
  URL: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsdm

- W3C XML Encryption
  URL: http://www.w3c.org/Encryption/2001

- W3C XML Digital Signature

  URL: http://www.w3c.org/Signature

- OASIS SAML

  URL: http://www.oasis-open.org/home/index.php

- OASIS XACML

  URL: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

- OASIS WS-Security Specification
  URL: http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf

- W3C XKMS (XML Key Management Specification)

  URL: http://www.w3c.org/2001/XKMS/

- MS, VeriSign, IBM WS-SecurityPolicy (Web Services Security Policy Language)

  URL: ftp://www6.software.ibm.com/software/developer/library/ws-secpol.pdf

- MS, VeriSign, IBM WS-Trust (Web Services Trust Language)

  URL: ftp://www6.software.ibm.com/software/developer/library/ws-trust.pdf

- MS, VeriSign, IBM WS-Federation (Web Services Federation Language)

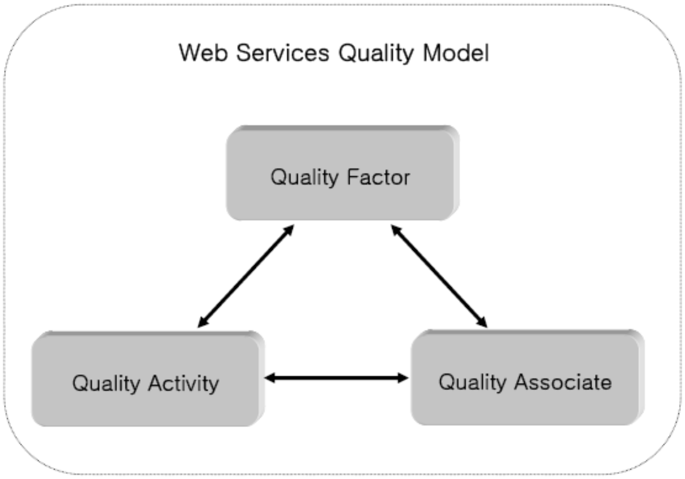
  URL: ftp://www6.software.ibm.com/software/developer/library/ws--fed.pdf

2.2 Acronyms

- ISO: International Standard Organization
- BLA: Business Level Agreement
- SLA: Service Level Agreement
- SOAP: Simple Object Access Protocol
- WSDL: Web service Description Language
- UDDI: Universal Description, Discovery and Integration
- XML: eXtensible Markup Language
- 2PC: 2 Phase Commit
- ACID: Atomicity, Consistency, Isolation and Durability
- WSDM: Web services Distributed Management
- HTTP: Hyper Test Transfer Protocol
- SSL: Secure Socket Layer
- TLS: Transport Layer Security
- IPSec: IP Security
- DOS: Denial of Service
- IDS: Intrusion Detection Service
- IPS: Internet Protocol Security
- S/MIME: Secure / Multipurpose Internet Mail Extension
- PGP: Pretty Good Privacy
- MIME: Multipurpose Internet Mail Extensions
- XML-DSIG: XML Digital Signature Standard
- PKI: Public Key Infrastructure
- XKMS: XML Key Management Specification
- SAML: Security Assertion Markup Language
- XACML: Extensible Access Control Markup Language

3 Web Services Quality Model

Web Services Quality Model configures major components of Web Services and presents a milestone for the quality of service level. As shown in <Figure 3-1>, the Web Services Quality Model consists of 3 components: Quality Factor, Quality Associate, and Quality Activity. The Quality Factor is a fundamental component that recognizes Web Services quality to manage its quality. The Quality Associates refer to roles or tasks of the organizations or people related to Web Services. And the Quality Activity refers to various action models performed by Quality Associates for the stability of Web Services quality. The Web services Associates MAY require any necessary contracts while interacting with one another. So, the suggested model focuses on consolidating the necessary Quality Factors for Web Services quality incurred from Quality Activity.



<Figure 3-1> Web Services Quality Model

The Web services Quality Model illustrated in <Figure 3-1> refers to Quality components and their relationships. Since most of Web services are remotely provided, Web Services quality has its significance when the quality in remote services is fully considered.

The Quality Associates are the organizations or people related to inspection, loading, provision and use of Web services. The associates could be developers, providers, users and managers of Web services. Depending on their interests, they have different views regarding Web services quality. Their quality contracts are concluded through negotiations, based on quality model instance of their own viewpoint.

The Quality Activity configures various activities of Web services such as contracting among Quality Associates. There are three types of the Quality Contract: 1) Employment Contract, 2) Development Contract, 3) Management Contract. Development Contract is a contract between Stakeholder and Developer at the time of development consignment. Employment Contract is a contract between Provider and User for quality guarantee. Lastly, Management Contract is a contract about Web Services quality required for its management when Stakeholder consigns its management to a dedicated management facility.

3.1 Quality Factor of Web Services

Web Services is regarded as a product remotely used, so the quality of Web Services should be reviewed when they are used in remote site.

3.1.1 Web Services Quality as a Service

Web Services are provided as a service, not the product itself. Considering the service-oriented features of Web Services, Web Services Quality Model should be established from the view of service quality, not the product.

3.1.2 Quality Service Model

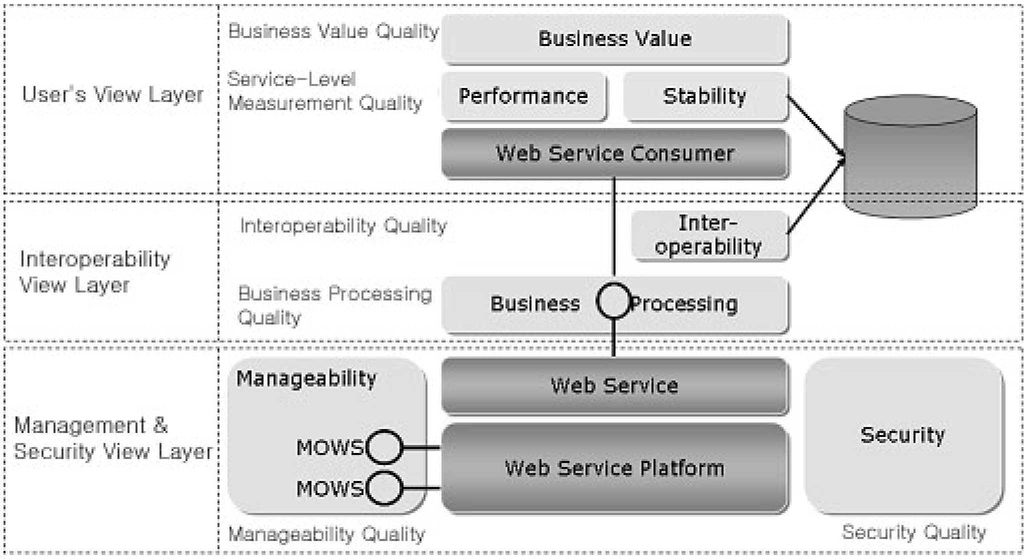
Web Services quality as a service is literally the quality of using Web Services and depending on the views of using a service, it can be considered in three layers; 1)Business Level Layer, 2) Service Level Layer, 3) System Level Layer. Each layer has one or several quality sub-factors (see Figure 3-2).

The first layer, Business Level Layer is the quality to represent the business value perceived by the user while using Web Services and is called Business Value Quality.

The second layer, Service Level Layer is the measurable performance quality of Web Services perceived by the user while using Web Services and is called ‘Service-Level Measurable Quality.’ This quality includes performance issues such as stability and scalability as well as response time. The quality factors at the user level layer can be obtained by evaluating the service quality that User experiences while using Web Services.

The third layer is the System Level Layer. This layer can be divided into 'interoperability layer' and 'management and security layer'. Interoperability layer is the layer that determines whether Web services, which are developed in different system environments by different developers, can properly interoperate. The quality of this layer can be subdivided into two types of quality depending on the user's interest. One is the quality of whether message format among Web Services is exchangeable, that is, whether the format conforms the standard and/or guideline specified by standard organizations, called Interoperability Quality. Another one is the quality of whether the interoperating messages properly execute business logic, called Business Processing Quality. This can be subdivided into 'Reliable Messaging' for stably delivering at any unstable networking situations and quality factors for properly executing a desired ‘Business Context’. The quality at interoperability view layer can be obtained by evaluating 'message log information', which is saved by intercepting a message in the middle of exchange between Web Services and 'message processing status log information', which is saved while a message is being processed. Management and security layer is a layer to indicate the quality from the management and security view of Web Services and can be divided into the manageability quality and security quality. Manageability Quality is the quality to indicate the manageability from within or outside of the system. Security Quality is the quality to indicate the level of the counteraction of Web Services to the unauthorized access or attack from outside. The manageability and security layer quality can be checked by testing the manageability and security related features.

<Figure 3-2> illustrates the concept of 6 major quality factors that belong to the three layers mentioned above.



<Figure3 -2> Web service Quality Factors

3.2 Quality Associates for Web Services

A Web service quality associate is the person who is related to each step of Web services life cycle such as stakeholder, inspection, loading, provision and use and its related system. The Quality Associate is namely the model of these stakeholders suggested in the draft. <Figure 3-3> illustrates the relation between the web quality stakeholders and their quality contracts, which are concluded due to necessity.

3.2.1 Stakeholder

A Web service stakeholder is the main body who requests the development of a Web service to a developer and user who has the authority to place an order related to Web services development. A stakeholder delivers the requirements of Web services quality to a developer when requesting the development. That's because a stakeholder has an expectation as to what quality level a Web service is developed. The quality requirements should be prepared before development.

3.2.2 Developer

The developer considers the Web services quality requirements that will meet the quality standard and designs the structure to meet the quality accordingly. A stakeholder uses the quality models while testing whether a Web service meets the quality level, which is specified in the quality requirements. Testing the quality is called 'Quality Inspection Procedure'

3.2.3 Provider

A Web service provider is also a user who provides the existing Web services or a new Web service independently developed by the provider. The Web services quality has an important meaning on the provider's side because the provider's company will lose profits if a competitor provides better quality service to the stakeholder. Therefore, it should be focused that a Web service is developed and managed so that a better quality would be provided by measuring quality more accurately on a Web service provider's side.

3.2.4 Consumer

A Web service consumer is a user who actually uses the Web services. It is understood that a customer is also most closely related to Web services quality because a user and a consumer selects the highest quality service in case there are several available Web services. Therefore, the method to define the accurate quality class and level concerning Web services quality should be provided to the consumer. Consequently, it can be said that the choice whether or not to use a Web service depends directly on the quality.

3.2.5 QoS Broker

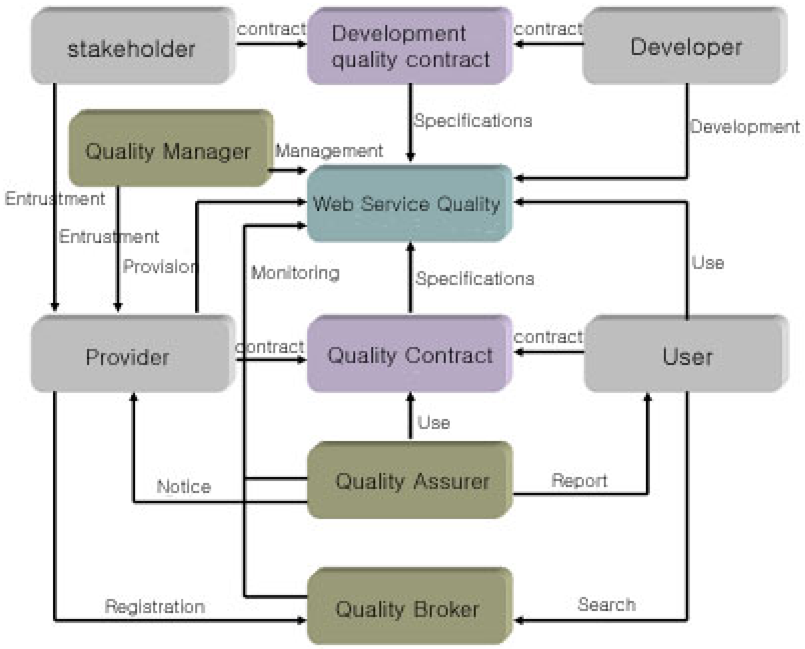
On the Web services user's side, most users expect to get the highest quality Web service. A QoS Broker saves Web services information, especially concerning the quality in order to search appropriate quality information among the registered Web services when any quality-related request is accepted and provide a user with the Web services suitable for the user's requirements. Like this, a QoS Broker registers Web services quality properties using the Web services quality model suggested in the draft when registering a Web service. In addition, a QoS Broker monitors whether a registered Web services provides the registered quality level. The quality models are used when a QoS Broker monitors the quality properties.

3.2.6 Quality Assurer

A quality assurer functionally monitors the quality level to see whether or not the quality level contracted between a Web service provider and a Web service user is well kept and provided. The quality contract is called the 'Quality Contract of Web services', which uses the quality model of Web services when creating, loading and using a quality contract. In addition, a quality assurer monitors whether or not a Web service is provided at its contractual quality level, whether or not a quality contract of Web services is observed and whether or not a violation related to quality level is notified/recognized between the Web service provider and the Web service user.

3.2.7 Quality Manager

A quality manager plays a role to carry out the management service of a Web service provider as proxy. To secure the quality level requested by the provider, a quality manager monitors the system from the outside and manages Web services quality. The quality management service also contains Web services resource management in order that a Web service is continued with reserved resources even in case system resource is insufficient. A quality manager should secure a system to control plural Web services and be a group or public enterprise with public trust by which a Web service provider can carry out such services.



<Figure 3-3> Quality Associates of Web services

3.3 Quality Activity of Web Services

Quality Activity consists of various activities to make a contract for the stability of Web Services Quality among Quality Associates. The followings indicate the list of its activities.

● Contract

It is cooperation among associates with the details of Quality Development, Quality Usage, and Quality Management for the quality stability

● Clarification

It is an activity of defining the details of Web Services Quality and the Quality Level for clear understanding at the time of contract.

● Search

It is a User's activity of searching for the quality detail or the superior quality web service.

● Delegation

It is a Provider's activity of delegating the quality monitoring or the quality management to maintain its quality level.

● Development

It is a Developer's activity of designing, coding, testing and integration with quality in mind at the time of Web Services Development.

● Registration

It is a Provider's activity of publishing its quality detail and quality level to Quality Broker.

● Report

It is a Quality Assurer's activity of reporting to User about the usage history of quality information and any violations in Web Services Quality Level based on its quality contract.

● Notification

It is a Quality Assurer's activity of notifying Provider about any violations in Web Services Quality Level based on its quality contract.

● Monitoring

It is a QoS Broker's activity of monitoring Web Services Quality Level on a regular basis. (Daily, Monthly, Yearly)

● Management

It is a Quality Manager's activity of managing quality to assure the Quality Level requirement of Provider.

Contract is most important in Quality Activity. There are three contracts related to Web Services Quality. The first is a Development Quality Contract between its Developer and Stakeholder. The second is Web Services Quality Contract in User's perspective between its Provider and User. The last is Management Quality Contract which should be maintained when Owner (Stakeholder) delegates Web Services management to a dedicated management facility (Provider) instead of managing it directly.

3.3.1 Development Quality Contract

Development quality contract means a quality contract at the Web service development stage. Tasks at Web services development stage include design, implementation, unit quality test and integration test of services. Each task can be influenced by plenty of factors. In order to assure that a Web service is developed at the required quality level, a developer should consider the quality at each task and test the quality of Web service. A stakeholder should evaluate a Web service that is developed by a developer and inspect it accordingly. Therefore, the development quality contract of Web services should contain the detail specifications to be attained in the development and the inspection checklist to be consequently executed.

3.3.2 Web Services Quality Contract

The Web services Quality contract should be concluded between a Web service provider and a user at the time of starting the use of such Web services. This means that a Web services quality contract is prepared through a discussion &/or negotiation about functions and quality of Web services provided in the presence of the 3rd party. In general, a Web services quality contract describes functions to be provided to a provider by Web services, quality items to be provided at the time of using such services, warranty level and corrective actions in case of any violation. These contracts are business-level agreement, business contract and Service Level Agreement (SLA) related to XML, an electronic document format to be used for quality control that Web service management platform is understandable. The latter, service-level agreement is also called WS Quality Contract or more simply, WS-Contract. Upon the preparation, the SLA is distributed to service providers, consumers and platform of a quality manager and used at the stage of using Web services. Therefore, a Web services quality contract should contain items to be considered about Web service quality from the view of using such services.

3.3.3 Management Quality Contract

Management Quality Contract is a contract between Web Services owner and Provider when Web Services owner (Stakeholder) delegates the management and supply of Web Services to a dedicated operator instead of managing it directly after the development of Web Services is completed. This contract is about the essential qualities which should be supplied to User by Provider for maintaining Web Services Quality. Its conformance can be evaluated through monitoring by other Quality Manager or Quality Assurer.

4 Business Value Quality

4.1 Definition

Business Value Quality means differentiating business value from the viewpoint of using Web services, that is, at service level of Web services. Business value of Web services MAY supplement with business profits or elevate service quality remarkably.

4.1.1 Type

Business Value Quality doesn't exist independently. It has to consider all the elements in quality standard, and the type and characteristic of current business. And it can be classified as shown below. When choosing service, the appropriateness of its service is determined and the output from its service is measured and evaluated. Quality of Service can be evaluated by these methods with better recognition. The followings are detailed definitions in regard to Quality.

● Business Suitability

It is a property to determine the suitability of business implementation using its service when conducting a business. It is evaluated in business perspective and IT perspective.

- Business perspective

Business Suitability is evaluated after checking necessary elements (Business for its service, Importance of ongoing business, Need for service) to conduct the business.

- IT Service Perspective

The evaluation is done from different angles including ease of use, efficiency, and stability.

● Business Effect

It is a property to show the outcome from implementing Provider's Web Services in business. It is crucial element to calculate the business value. Due to its influence on Business Suitability, Business Effect can be a reference when using services in other businesses. It also plays an important role to create Web Services recognition along with offline survey.

● Business Recognition Level

It is a property to indicate the level of the recognition of Web Service. It shows the level of reputation and application of Web Services implemented by User in business and the service category of its business can be created through the recognition level of each business area.

4.2 Quality Sub-factors

Business value quality consists of 3 quality sub-factors as follows.

4.2.1 Business Suitability

● Business Suitability

It is a property to evaluate the suitability with the industry standard that belongs to the business category and the business requirements of Web Services. Business Suitability is the measurement to evaluate the business level indicated on BLA (Business Level Agreement) and the suitability of business implementation between Provider and the service. Higher the suitability is, it's more likely for the business optimization of Web Services to occur. Business Suitability is regarded to have three fundamental elements as follows but the expanded elements can be used to evaluate the suitability.

- Applicable area for Services:

It is to describe the business category classification which should include the service from Provider. And the location of its business category (manufacturing, finance, public industry, etc.) can be designated

- Need for Services:

It is a part to describe the reason of the service to be used in business. And the solution for the existing business problem is proposed or the reason for applying the service onto the business is indicated.

- Importance of applicable business:

It is a property to indicate the importance of business in which the service of business category (manufacturing, finance, public industry, etc.) is used. For example, the production part of manufacturing business can be an important factor but HR or general affair are relatively less important.

● IT Service Suitability

It is a provider's property of Provider to evaluate the ease of use of Web Services. If the feature of Web Services doesn't distinguish each other, Web Services with better ease of use is rated for better suitability

4.2.2 Business Effect

● Business Activity Contribution

It is a user's property to evaluate the contribution in its business profit when using business friendly service. It also can be used as a data to calculate ROI (Return On Investment) High Business Activity Contribution can be interpreted as high ROI.

● Business Activity Influence

It is an evaluation factor for the influence on the business when the service with low optimization is used for Web Service user. High business activity influence means that it can be classified as the common service regardless its business classification and for the case like this, it can be defined with the classification of common service and optimized service while specifying a specific level.

● Customer Satisfaction Effect

It is a property to evaluate the satisfaction after using the Web Service. Web Service user can measure it using the survey and real-time monitoring. The high customer satisfaction likely means the high reputation of Provider's Web Service.

● Return On Investment Effect

It is a user’s property to evaluate the profit on investment with financial result. It is possible to calculate through Business Activity Contribution, Business Activity Influence, and Customer Satisfaction Effect.

4.2.3 Business Recognition Level

● Reputation

It is a reputation of Web Services from customers. Reputation is evaluated by Quality of Service, level of satisfaction, and reliability. It can be measured with various method such as survey and vote, etc.

4.3 Quality Contracts

Service level business value quality-related quality contracts are as follows.

● Quality Contract for Development

Of business value quality factors, the quality sub-factors such as metering/billing should be contained in a BLA development quality contract. BLA is an agreement describing what kind of service is provided, that is, from the view of business.

● Quality Contract for Using Web services

If a consumer is willing to use a Web service, the consumer can review the cost, penalty, metering and billing, which are described in WSDL. Meanwhile, a QoS broker should test every quality sub-factor of business value quality on/off line and expressly indicate the quality.

4.4 Quality Associates

● Stakeholder: is interested in every quality factor related to business value quality.

● Developer: is engaged in metering/billing.

● Consumer: is interested in every quality factor related to business value quality.

● Provider: should make an effort to win recognition of a good business value quality.

- QoS Broker: should collect and give business value quality information through online/offline questionnaires or voting to consumers in order to publicize the information to the public.
- Assurer: N.A.
- Manager: N.A.

4.5 Related Standard

N.A.

5 Service Level Measurement Quality

5.1 Definition

Service Level Measurement Quality is the quality that a user perceives when actually using Web services. The quality generally means how fast a Web service is provided and/or how stable it is provided, all of which are measurable at all times.

5.1.1 Type

Performance related quality sub-factors include Response Time, Throughput, and Maximum Throughput and Stability related quality sub-factors include Availability, Reliability, and Accessibility.

5.2 Quality Sub-factors

Service Level Measurement Quality is subdivided into performance measurement sub-factors including response time, throughput and maximum throughput, and stability measurement sub-factors such as availability, reliability and accessibility. The followings define the quality sub-factors.

5.2.1 Performance

Of the Service Level Measurement Quality, the performance-side property is how fast a Web service provider responds to any service request. The performance property can be described in quality sub-factors such as response time, throughput, and threshold quality.

● Response Time

It means the time taken to send a request and to receive the response. The Response Time is measured at an actual Web service call and it can be calculated by applying the following formula. The Response Completion Time is the time that all the data for response arrives at a user, while the User Request Time is the time when the user sends a request. In general, the Response Time is calculated by the mean value during a certain time.

$$\boxed{\text{Response time} = \text{Response Completion Time} - \text{User Request Time}}$$

● Maximum Throughput

It means the max number of services that a platform providing Web services can process for a unit time. Throughput can be used as a performance index to evaluate a Web services provider. How many it can process also means how many users it can process concurrently in a web. The Maximum Throughput can be calculated with the following formula.

$$\text{Maximum Throughput} = \frac{\text{max } \textit{complete requests}}{\textit{unit time}}$$

5.2.2 Stability

Stability means how stable and continuously Web services can provide services. That is, the quality is about the ability to provide continuous, consistent and recoverable services despite of increased throughput, congestion, system failure, natural disaster and intentional attack from users. The quality properties are availability, reliability and accessibility.

- Availability

Availability is defined as the ratio of time period in which a Web service exists or it is ready for use, that is, the Web service is maintained. Assuming that the time when a system is not available is 'Down Time' and the time when a system is available is 'Up Time,' the Availability is the average Up Time. To get Availability, instead of monitoring Up Time continuously, we suggest using the Down Time. Down Time could be obtained by monitoring system down events occurred in operation. The following formula calculates the Availability while unit time is a time to measure the time.

$$Availability = 1 - \frac{Down\ Time}{Unit\ Time}$$

- Successability

Successability is defined as the extent to which Web services yield successful results over request messages. Successability means the degree to which a service is fulfilled in a given time according to an agreed contract. Successability can be calculated as the number of successful response messages over the number of request messages. That is, it represents the ratio of successfully returned messages after requested tasks are performed without errors.

$$Successability = \frac{number\ of\ response\ messages}{number\ of\ request\ messages}$$

- Accessibility

Accessibility represents the degree that a system is normatively operated to counteract request messages without delay. In some cases, a Web service system could be accessible for external users to try accessing its resources even if its services are not available. We can know whether a Web service system is accessible by just inspecting that the system can returns an acknowledgement normally for a request message. Thus, Accessibility can be calculated as the ratio of number of acknowledgements received to the number of request messages.

$$Accessability = \frac{number\ of\ acks\ received}{number\ of\ request\ messages}$$

5.3 Quality Contracts

- Quality Contract for Development

The quality level in each quality factor SHOULD be described in the BLA (Business Level Agreement) and the SLA (Service Level Agreement), which are made when development is ordered. SLA is a contract document specifying the quality level of a Web service(s) provided, the relative details and the corrective measures in case of any violation against the described quality level.

- Quality Contract for Using Web services

When services are used, the quality level in each quality factor SHOULD be described in BLA and SLA. QoS broker, quality assurer, and manager SHOULD monitor and check whether quality contracts and the specified quality are properly maintained.

5.4 Quality Associates

- Consumer

Web services consumers wish to use high-performance and stable Web services, so they are even more interested in service level measurement quality than any other qualities.

- Stakeholder

A stakeholder also desires to have a Web service of service level measurement quality when requesting a Web service development. Like the reasons why consumers are interested in Web services, stakeholders have also intent to manufacture high quality Web services more consumers can use.

- Developer

A Developer should develop a Web service that meets the quality level designated by a stakeholder as the same reason why the stakeholder is interested in service level measurement quality. In an inspection time, the developed Web service should pass the quality level test specified in a development contract.

- Provider

A Provider should manage a platform to provide Web services, while maintaining its quality level specified by a stakeholder. On the Provider's part, service level measurement quality is one of important factors among service qualities like web hosting.

- QoS Broker

Among the Quality Associates, QoS (Quality of Service) Brokers provide the most objective measurement and criteria of service qualities. QoS broker can measure service level measurement quality more accurately than any other quality and search a Web service suitable for a user more easily.

- Assurer

See QoS Broker

- Manager

See QoS Broker

5.5 Related Standards

- N.A

6 Interoperability Quality

6.1 Definition

Interoperability Quality defines the compatible/inter-operable level among Web services. Since Web services that are defined on different platforms and of which standard specifications are individually extended and defined, it occasionally happens that additional development for interoperability among these services is not easy, although the technologies of Web services have been standardized. Therefore, interoperability quality means the results of evaluating the interoperability level by a specific standard, which is required for inter-operation among Web services.

6.1.1 Type

Interoperability Quality includes the conformability of SOAP, WSDL, and UDDI as Quality Sub-factors.

6.1.2 Quality Sub-factors

Interoperability Quality can be divided into Conformability and Interoperability.

6.2 Quality Sub-factors

- Conformability

Standard Conformability is a factor to evaluate to which degree the standard technology of Web services are conformed. From the view of standard conformability, the interoperability quality evaluation inspects whether a Web service implemented reflects the standard specifications.

- Interoperability

Interoperability is a factor to evaluate whether both conformable Web service systems are interoperable according to a WS-I profile, which is the authority to define interoperability of Web services and suggest profiles of Web services specifications. The profile suggests the guidelines of the applicable Web services standard.

6.3 Quality Contracts

- Development Quality Contract

Interoperability quality contract in development should contain quality factor, which is required by BLA [Business Level Agreement]. The level of interoperability quality can be evaluated by the test of interoperability suggested below.

- Operation Quality Contract

A Web service is provided to users [consumers] through UDDI storage after being evaluated for the service quality by the 3rd quality certificate authority and receiving the quality certificate.

6.4 Quality Associates

● Stakeholder

When placing orders of Web services to several companies, a Stakeholder should consider the interoperability quality of Web services developed by different companies and supply them.

● Developer

A Developer should consider the interoperability with other Web Services when developing Web Services

● Provider

A Provider should provide Web Services that assures the interoperability quality.

● Service Consumer

A Service Consumer should use a Web service to which the interoperability quality is secured.

● QoS Broker

QoS Broker should keep the information on Web services interoperability quality with Web services information, search the interoperability quality information of Web services when a request for quality occurs and provide users with a Web service suitable for the required conditions.

● Quality Assurer

A Quality Assurer should assure the quality by monitoring to see that the interoperability quality is provided based on the contract between Provider and User

● Quality Manager

A Quality Manager should monitor and manage a system remotely for the assurance of interoperability quality required by Provider.

6.5 Related Standards

● WS-I Basic Profile 1.1: this is the interoperability profile for SOAP, WSDL, UDDI standards and is managed by WS-I. ▪

URL: http://www.ws-i.org/Profiles/BasicProfile-1.1-2004-08-24.html

● WS-I Basic Security Profile Version 1.0 : this is the interoperability profile of Web service security and is also managed by WS-I. ▪
URL: http://www.ws-i.org/Profiles/BasicSecurityProfile-1.0-2004-05-12.html

● WS-I Simple SOAP Binding Profile Version 1.0 : this is the interoperability profile of SOAP binding and is also managed by WS-I. ▪

URL: http://www.ws-i.org/Profiles/SimpleSoapBindingProfile-1.0-2004-08-24.html

7 Business Processing Quality

7.1 Definition

Business Processing Quality means various indices to provide optimized business when business partners execute the business process for Web services. The provision of such optimal business requires accurate definition, execution, automation of business process, reliable messaging, transaction processing, coordination and integrated management framework.

7.1.1 Type

Quality Sub-factors of Business Processing Quality can be divided into three. The first is to monitor the reliable processing and escape sequence status. The second is to assure the transaction of single task using multiple business processes. The last is to check the conformation of predefined process, and to design a framework for modeling and adjusting the distributed business processes. Thus, to process the business processing quality, the following two requirements must be satisfied first: 1) Reliable Messaging and Transaction of business message, 2) Business process collaboration of process management

● Reliable Messaging

It is ability of Web Services to check the message transmitted through networks on Internet where unreliable messages occur. It refers to the retransmission in case of lost messages with unique identifier and sequence number assigned by various OS and middleware systems.

● Transactionality

It is ability to process multiple messages among participants into single logical entity while the multiple message sets are exchanged among many participants in complex business scenarios.

● Business Process Collaborabillity

It is ability to process Web Services workflow. It refers to the business collaborability to combine, design and implement Web Services and business process for the desired process outcome. In general, the business collaborability is accompanied by many business activities. The changes and order of these activities need to be defined according to the standard and the business process would be able to be executed by such a defined process.

7.2 Quality Sub-factors

Quality sub-factors of business processing quality can be divided into two; one is to organize a framework for modeling and adjusting diversified and distributed business process and the other is to monitor observation of predefined process procedure, reliable processing and exceptional process status. Therefore, for satisfying the business processing quality, there are two important factors: 1) the reliability of business messages, 2) elaborate transaction and process management on the message context properties. The following shows the definition of each component.

7.2.1 Reliable Messaging

Reliable messaging represents the property of whether the most reliable message is supported for business processing. For the reliable messaging, a message that is duplicated or fails transmission should be retransmitted to secure business processing quality. In general, reliable messaging should guarantee the properties of AtMostOnce, AtLeastOnce, ExactlyOnce and InOrder. OASIS presented WS-Reliability and WS-ReliableMessaging specifications for the properties. The followings list the criteria of reliable messaging.

- AtMostOnce: a transmitted message should be delivered once at most.
- AtLeastOnce: a transmitted message should be delivered once at least.
- ExactlyOnce: a transmitted message should be delivered exactly once.
- InOrder: to be transmitted, messages should be delivered in transmitted order.

7.2.2 Message Context

A business process could include execution of distributed Web services. For the coordination and transaction processing among these distributed services, a system requires the history information shared by participating transactions from the start time to the end time. A message context contains the information shared by all the resources for a participating transaction, which is created when the transaction starts and deleted when it ends.

7.2.3 Transaction

Transaction is a set of tasks that should be processed as a group at once. In general, it should satisfy the following 4 properties.

- Atomicity: all operations occur if successful while no operations work if failure.
- Consistency: application executes effective status conversion upon the completion.
- Isolated: operation results are not shared outside a transaction until it completes successfully.
- Durability: once a transaction has been successfully completed, a failure can be recovered.

A Web service transaction could be categorized as ‘atomic transaction’ recognized as general meaning and ‘business activity.’ Business activity has more complicated interests and a longer transaction period than the atomic transactions. The former is realized frequently by using 2PC(2-Phase Commit), while the later uses compensation for failures. Transaction processing in Web services environment may be implemented by using WS-Coordination/WS-Transaction specification. WS-Coordination contains the protocol for transaction coordination and transaction processing scenario and WS-Transaction includes the definition of two type of transaction and these scenarios.

● Short-Term Atomic Transaction

Atomic transaction, as the basic transaction, has a narrow transaction range and a short transaction processing period. Until a transaction is operated and complete, it completes cooperation with any other participants and exchanges messages with them, during which transaction information is shared through a coordinator and monitored subsequently. Such a transaction is finalized through 2PC.

● Long-Term Business Activity

The business activity is a long term transaction and covers transactions that may not be processed by atomic transactions. Business activity may not always meet the ACID property which is the basic requirement of a transaction. 2PC blocks the other user's access to data used in an atomic transaction before commit. On the contrary, business activity cannot restrict other user's access in its long execution time. So, the compensation process, which recovers partially process result to the previous step in a failure, is necessary mechanism in the business activity.

● Centralized Business Process Management

Centralized business process management creates, executes and monitors a new business process as a part of work-flow by combining several Web services, which are provided by many Web service providers. And it should provide a convenient automation level to organize new Web service registration, service creation, role definition (regulator, participants), calling protocol definition and execution environment.

● Decentralized Business Process Management

In the decentralized business process management, managing business processes distributed as fragments in Web service environment is not centralized but distributed in their actual regions of each process for the management.

7.3 Quality Contracts

● Quality Contract for Development

A business process quality contract in the development should describe test items in BLA (Business Level Agreement) by quality factors while the business processing quality level is evaluated by test by each factor.

● Quality Contract for Using Web services

A Web service is provided to users [consumers] after being evaluated for the service quality by the 3rd quality certificate authority and receiving the quality certificate.

7.4 Quality Associates

For the business processing quality, each quality associate is interested in the followings.

● Developer

A developer should assure Reliable Messaging and Transactionality considering the business collaborabililty with other Web Services at the time of development. And a developer also needs to design, define and develop a workflow precisely for the business processing.

● Service Consumer

A consumer is a user who actually uses Web service business processing service. A consumer should select a high quality service referring to business processing quality certificates.

● Service Provider

For service providers, the business process quality is one of important factors for the business competitiveness. A provider should do their best to insure that each test item for the contractual business processing quality receives higher implementation. It is also focused to develop a service, which provides higher quality through the quality test.

● QoS broker

A QoS broker inspects business processing quality in order to confirm the quality level when a provider registers a Web service quality certificate. With the business processing quality test results, the quality level is determined according to the test results executed by a broker in case a consumer asks a QoS broker to search a Web service.

● Stakeholder

A stakeholder is a main body to commit a service to a business partner and an owner who has the authority to order services. A stakeholder delivers the requirements of the Web services business processing quality when requesting a service development. He also inspects the quality whether the quality requirements are kept according to the described quality level.

● Quality Assurer

A quality assurer monitors Business Process Quality level between the provider and user and performs a quality assurance activity such as issuing Web Services Quality certificate.

● Quality Manager

A consumer is a user who actually uses Web service business processing service. A consumer should select a high quality service referring to business processing quality certificates.

7.5 Related Standards

● OASIS WS-Reliable Messaging: defines messaging protocols of checking, tracing and managing messages to insure that messages to be transmitted among business partners are reliable.

URL: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsrm

● OASIS BPEL4WS(Business Process Execution Language For Web service): defines a sequence that several business processes are executed in Web service environment.

URL: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsbpel

● IBM WS-AtomicTransaction: defines Atomic Transaction for processing short-term transaction

URL: http://www-128.ibm.com/developerworks/library/specification/ws-tx/#atom/

● IBM WS-BusinessActivity: defines Business Activity for processing long-term transaction

URL: http://www-128.ibm.com/developerworks/library/specification/ws-tx/#ba/

● IBM WS-Coordination: provides Web services-based approach to improve the performance of long term business transactions, which are automated in an expandable and interoperable method.

URL: http://www-106.ibm.com/developerworks/library/specification/ws-tx/#coor

● OASIS WS-CAF(Composite Application Framework): is the standard to support a service necessary for integrating business processes of Web services.

URL: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ws-caf

● W3C WS-CDL (Web services Choreography Description Language): describes a coordination of XML-based Web services and specifies distributed business process management.

URL: http://www.w3.org/TR/2004/WD-ws-cdl-10-20040427/

8 Manageability Quality

8.1 Definition

Manageability quality is the quality in the viewpoint of a manager or Web services tool developer. That is, it means the quality to be managed by using object properties such as the relationship among objects, identification, status and structure information, operation and events to manage the Web services system.

8.1.1 Management Functions

The Manageability quality could be maintained by three functions of a management system;

- Introspection: to inspect system and system's internal information
- Control: to control writes to system and system's internal information
- Notification: to notify, if any, changes in internal information.

● Introspection: to get information on the classes of Web services, resources, and their status. The information also contains Web services tracking information, that is, through which route a Web service is called.

● Control: to manage Web services and resources including the information obtained by introspection and the manageability of Web services objects and resources. While Introspection merely gains information, this function obtains and manages such information.

● Notification: to notify changes in Web services or resources, if any, to an external quality manager or anyone who wishes to know it.

8.1.2 Manageable Services

● Web service Management: It's the management of Web service itself. A service should have standard management interface, to be a manageable Web service.

● Web service Platform Management: it's the management of platform on which a Web service is installed and provided. It is available as long as such a platform is with the standard management interface.

8.1.3 Management Level

● Manageable Level: a Web service of manageable level is a service that provides management interfaces.

- Managed Level: a Web service of managed level is a Web service that is manageable and currently managed by the management interface

8.2 Quality Sub-factors

It defines the quality sub-factors, that is, 6 manageable levels and 2 managed levels by combining 3 functions and 2 manageable services described in 8.1.

8.2.1 Manageable Level

- Introspectability of Web services: introspectable Web service
- Control-ability of Web services: controllable Web service
- Notifiability of Web services: notifiable Web service
- Introspectability of Web service platform: introspectable Web service platform
- Control-ability of Web service platform: controllable Web service platform
- Notifiability of Web service platform: notifiable Web service platform

8.2.2 Managed Levels

- Introspectability of managed Web service: a Web service that is manageable and is managed by a manager for introspectability.
- Controllability of managed Web service: a Web service that is manageable and is managed by a manager for controllability
- Notifiability of managed Web service: a Web service that is manageable and is managed by a manager for notifiability
- Introspectability of managed Web service platform: a Web service platform that is manageable and is managed by a manager for introspectability
- Controllability of managed Web service platform: a Web service platform that is manageable and is managed by a manager for controllability
- Notifiability of managed Web service platform: a Web service platform that is manageable and is managed by a manager for notifiability

<Table 6-1> shows the above-mentioned quality sub-factors in a table.

<Table 6-1> Quality Sub-factors of Manageability

Level	Object	Introspectability	Controllability	Notifiability
Manageable level	Web services	Introspectability of a Web service	Controllability of a Web service	Notifiability of a Web services
	Web services platform	Introspectability of a Web service platform	Controllability of a Web service platform	Notifiability of a Web services platform
Managed level	Web services	Introspectability of a managed Web service	Controllability of a managed Web service	Notifiability of a managed Web service
	Web services platform	Introspectability of a managed Web service platform	Controllability of a managed Web service platform	Notifiability of a managed Web service platform

8.3 Quality Contracts

- ● Development Quality Contract

Manageability is included as one of requirements when a Web service is ordered to a developer. That is, manageability in development is contained as functional requirements in a development contract.

- ● Quality Contract of Using Web services

The manageability quality exposes a management function as a service type to be called. Therefore, the manageability quality is defined in WSDL (Web services Description Language) extended for manageability or so that a service is specified in WSDL. That's because the manageability should be exposed as a form of business Web service. Quality contract is also contained in BLA.

8.4 Quality Associates

- ● Consumer

No interest

- ● Stakeholder

A Stakeholder requests a developer to develop manageable Web services for obtaining the manageability quality described in a Web service development contract. In addition, a Stakeholder uses the manageability in the inspection procedure whether a developed Web service is manageable.

- ● Developer

A Developer implements Web services in the form that the manageability requested by a Stakeholder is to be contained in the Web services functions and guarantees the manageability quality in the inspection procedure. On a Developer's side, the manageability is accepted as one of Web services function requirements, independent from the above-stated service level measurement quality.

- ● Provider

A Provider SHOULD offer the manageability of a platform as well as the manageability of Web services. The platform manageability also contains a function to control the execution environment of the whole Web services.

- ● QoS Broker

No interest

- ● Assurer

No interest

- ● Manager

A Quality Manager uses management function of Web services to provide manageability quality. On a manager's side, the manageability quality is very important and the management service can't be executed unless it provides the manageability quality.

8.5 Related Standard

- ● OASIS WSDM: standard of 'Management Using Web service' and 'Management Of Web service'. URL: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsdm

9 Security Quality

9.1 Definition

Web services security quality is the ability to determinate the legality of access to the system and service, to cut off any illegal approach, fabrication and authority exercise, to control any legal access and to provide integrated security service for the use of stable, reliable and appropriate authority in order to reduce or eliminate all potential threats, which may occur while using Web services. In the Web services environment, the method for applying security service MAY be redefined in that for existing security standards because of access method and service interface shared by WSDL, SOAP message communication through XML, and the indigenous features implemented on various platforms.

9.1.1 Qualities of Security Services

The security service qualities for Web services MAY be classified as follows.

- ● Data Confidentiality

It is the quality used to protect data against unauthorized disclosure. It is whether the information stored on a system is protected against unintended or unauthorized access. Since systems are sometimes used to manage sensitive information, Data Confidentiality is often a measure of the ability of the system to protect its data. Accordingly, this is an integral component of Security.

- ● Data Integrity

It is the quality used to ensure that data has not been altered or destroyed in an unauthorized manner. Data integrity is verified by using the features of hash function but in case electronic signature is used, it may be also verified by using a property to verify data integrity contained in the signature.

- ● User Authentication

As a procedure in which assurance of the claimed identity of an entity is provided, a common authentication uses a specific knowledge that a requester can understand. In Web services environment, SOAP messages pass through various security domains, so it is required to provide single sign-on function using a security token.

- ● Access Control

As a security quality to restrict unauthorized user's access, access MUST be controlled by using Web services security token, since a SOAP message passes through various security platforms. eXtensible Access Control Markup Language (XACML), an OASIS specification for the Access Control, provides fine grained control of authorized activities, the effect of characteristics of the access requestor, the protocol over which the request is made, authorization based on classes of activities, and content introspection.

▪ ● Non-Repudiation

A quality that provides proof of the integrity and origin of data, both in an non-forgeable relationship, which can be verified by any third party at any time, or, in an authentication that can be asserted to be genuine with high assurance. A property achieved through cryptographic methods which prevents an individual or entity from denying having performed a particular action related to data.

▪ ● Accessibility

In the Web services environment, accessibility depends on the ability to detect and prevent any attack of DoS. The basis of accessibility is that every Web service user should have access to the information and experiences available online. In the broad sense, accessibility encompasses the capability to identify and obtain information, i.e., how easy is it to find needed information and retrieve it when you need it.

▪ ● Audit Trail

An audit trail leaves a log of attempted attacks to a specific service in order to utilize it as the data about vulnerability of Web services.

▪ ● Privacy

Privacy is the quality of a person to control the availability of information about and exposure of him- or herself. It is related to being able to function in society anonymously (including pseudonymous or blind credential identification). On both sides of Web services consumers and providers, it is the service for protecting disclosure of private information.

9.1.2 Security Service Level

Web services security mechanism can be layered in two levels as follows.

▪ ● Transport Level Security - Non-Persistent Level Security

Transport level security means the security within a sub-network layer of SOAP, Web services protocol. This uses SSL and TLS security mechanisms, which have been used on the existing web environment, and HTTP protocol. Since these types of transport level security do not support end-to-end security context, partial encryption and partial electronic signature, message level security is required to reflect those features. Especially, since transport level does not provide end-to-end security context, transport security is non-persistent level security in which any context information is lost once it has transmitted from a point.

▪ ● Message Level Security - Persistent Level Security

Message level security provides security services such as data confidentiality, integrity, authentication, non-repudiation, and access control on the basis of SOAP messages. Since the message level security provides end-to-end security context, it is persistent level security in which context information is maintained even though a SOAP message itself passes through various security domains.

9.2 Quality Sub-factors

9.2.1 Transport Level

In all, 16 quality sub-factors are identified by combining 8 security service qualities and 2 security service levels, defined in 9.1. However, because non-repudiation of transport level and privacy protection of transport level are not practical, we only specify newly 15 quality sub-factors by adding Single-Sign-On (SSO) service quality getting important in SOA environment of Web services.

- ● Transport Level Data Confidentiality

A secure network protocol, such as TLS [RFC2246] or IPSEC [RFC2402], provides transient confidentiality of a message as it is transferred between two adjacent Web services nodes.

- ● Transport Level Data Integrity

A secure network protocol such as TLS [RFC2246] or IPSEC [RFC2402] MAY be configured to provide for digests and comparisons of the packets transmitted via the network connection.

- ● Transport Level User Authentication

The authentication provided by the transmission channel of a message transmission layer may be unidirectional or bidirectional. For instance, TLS [RFC2246] or IPSEC [RFC2402] provides an authentication method to a sender so that a destination under TCP/IP may be authenticated. It can be implemented by using electronic signature method and a certificate issued by certificate authority may be also used.

- ● Transport Level Access Control

Transport Level Access Control is used to control a user's access to resources in a transmission channel and can be organized by using TLS or IPSEC protocol.

- ● Transport Level Accessibility

This prevents resources from being unavailable due to a DoS (Denial of Services) attack. This can be implemented through transmission-level packet monitoring by firewalls, IDS, IPS, etc.

- ● Transport Level Audit Trail

It creates and removes a session at the transport level, or leaves and audits a log after data transmission. Here, logging policy, that is, an appropriate pre-definition of contents to be utilized in an audit procedure is required.

9.2.2 Message Level

- ● Message Level Data Confidentiality

For the confidentiality for SOAP messages, XML-Encryption adopted as a standard in the W3C or WS-Security (OASIS Web services security specification) or other encryption procedures (for instance, S/MIME, PGP/MIME) may be used. Since XML-Encryption permits parts of the XML messages to be encrypted (or decrypted), it shows generally better performance than that of the encryption method at transport level when partial encryption is applied to the message.

- ● Message Level Data Integrity

This is for the data integrity at SOAP message level and can be realized by using XML-DSIG (XML Digital Signature) or WS-Security. XKMS (XML Key Management Specification) is a newer specification that significantly extends the PKI (Public Key Infrastructure) model by adopting XML to provide new levels of easy and interoperable key management service when XML-DSIG or WS-Security is applied.

- ● Message Level User Authentication

An electronic signature for SOAP head or body or payloads of a SOAP message can be generated and attached to the SOAP message using XML-DSIG standard adopted by W3C. Unlike the existing signature methods, the XML-DSIG can selectively perform signing of specific parts of an XML document and the signed part may be added to a document as long as the signature's effectiveness is guaranteed. By the XML-DSIG, several security services such as authentication, data integrity and non-repudiation can be also provided together. For user authentication, SAML (Security Assertion Markup Language) is also available. SAML is a framework for exchanging authentication and authorization information. Security typically involves checking the credentials presented by a party for authentication and authorization. SAML standardizes the representation of these credentials in an XML format called assertions, enhancing the interoperability between disparate applications.

- ● Message Level Access Control

Message Level Access Control enables the access levels to resources to be controlled by using the information contained in a SOAP message. It could be implemented by applying standards such as SAML and XACML. It may be also delivered with a message including the access authority defined by XACML in SAML, by which any user's access to resources may be controlled.

- ● Message Level Non-Repudiation

Message level non-repudiation can be realized by applying XML-DSIG and WS-Security implemented on PKI environment.

- ● Message Level Accessibility

This ensures accessibility to Web services against DoS attack to XML message. For implementing Message Level Accessibility, a SOAP Firewall could be used, which reliably protects against all the specific risks associated with the exposure of Web services across the company's firewall and the exchange of XML messages over external networks. It hides Web services behind virtual service endpoints and inspects all SOAP messages, blocking messages with incorrect, malformed, or malicious content.

- ● Message Level Audit Trail

This leaves and audits logs of each request/response message to call a Web service. Like transport level audit trail, the policy making to specify log contents for audit and trail should be preceded.

- ● Message Level Privacy Protection

As an end-user's privacy protection mechanism, there are specifications such as WS-Security, XACML and SAML for the data confidentiality and access control for a user's private information. WS-Policy, WS-Trust and WS-Privacy on the Web service security road map deliver privacy policies, reliance mechanism and privacy claims. WS-Policy, WS-Trust could be used for Privacy Protection but not only for it, and they are classified in this section because they are used in WS-Privacy. Once any privacy policy has been defined using WS-Privacy to WS-Policy context under WS-Security structure, a service to receive the message trusts and executes the defined policy.

- ● Single-Sign-On

A Single-Sign-On authenticates a user like the above Non-Persistent Authentication but it is different in that a single-sign-on is required because SOAP message passes through various security platforms. Single-Sign-On is achievable by using a security token issued by a reliable authority. It may be structured as a standard to implement portable trust such as SAML and be implemented by using solutions such as MS Passport, Liberty Alliance and etc.

9.2.3 Security Factors & Related Technology Mapping

The following <Table 7-1> shows the relationship between Web services security factors and the related technologies, which should be applied in order to meet such security factors.

<Table 7-1> Related Technology by Web service Security Factors

Security Factors	**Related Technology**
Transport level data confidentiality	TLS, SSL, IPSec
Transport level data integrity	TLS, SSL, IPSec
Transport level user authentication	TLS, SSL, IPSec
Transport level user access control	TLS, SSL, IPSec
Transport level accessibility	Firewall, IDS, IPS

Transport level audit trail	Logging, audit trail policy
Message level data confidentiality	XML-Encryption, WS-Security, XKMS
Message level data integrity	XML-DSIG, WS-Security, XKMS
Message level user authentication	XML-DSIG, WS-Security, XKMS, SAML
Message level non-repudiation	XML-DSIG, WS-Security, XKMS
Message level audio trail	Logging, audit trail policy
Message level access control	SAML, XACML
Message level accessibility	SOAP Firewall
Single-sign-on	SAML, Liberty Alliance, .NET Passport, WS-Federation
Message level privacy protection	WS-Policy, WS-Trust, WS-Privacy

9.2.4 Security Profile

Web services security may use several quality sub-factors, depending on the characteristics of application services. The values of the sub-factors are categorized in the 'Web Services Security Profile' (WS-SProfile) as a group of quality sub-factors that are frequently used together among these factors. The profile is used to set a security level with the other service partner and specified in a BLA (Business Level Agreement). Considering the number of security quality sub-factors, there could be a number of Web services security profiles. However, this specification defines 6 profiles that are presumed to be frequently used at present. More profiles MAY be added later if required.

- ● WS-SProfile 0

WS-SProfile 0 provides services such as authentication, message integrity, message confidentiality and access control using transport level security mechanism and secures accessibility against transport level DOS attack and etc.

The WS-SProfile 0 security protocols are TLS, IPSec and etc. TLS provides services such as user authentication, message integrity, confidentiality and an access control service with the functions of record protocol, handshake protocol, public key-based certificate creation and process, authentication mode support and etc between two applications. IPSec is, on the contrary, an open structure framework to provide security protocol based on IP layer in order to make up for secure communication between both far-ends and provides the security functions to support the weakness of IP. IPSec's primary security functions are authentication protocol(AH), encryption protocol(ESP), security linkage and policy database(SAD, SPD) and key management mechanisms, through which it can provide message integrity, message confidentiality and access control service.

- ● WS-SProfile 1

WS-SProfile 1 provides authentication message integrity, non-repudiation, and confidentiality by introducing electronic signature and encryption at message level. In some cases, security services such as message confidentiality and access control may use security mechanisms provided at the transport level but it is not essential.

The most representative standard of the WS-SProfile 1, WS-Security is based on SOAP, a Web services message exchange protocol, and adapted as the representative message level security technology to provide authentication, integrity, non-repudiation and confidentiality by OASIS in 2004.

XML-Signature and XML-Encryption of W3C have been extended and applied to WS-Security. WS-Security provides practical authentication, message integrity, non-repudiation and confidentiality at message level including time-stamp related functions to prevent replay attack, and it secures 'end-to-end transmission' of SOAP messages. WS-Security also supports various security tokens to exchange security information.

- ● WS-SProfile 2

WS-SProfile 2 provides access control service using message level access control mechanism, secures access against XML DoS attack using a SOAP Firewall and contains WS-SProfile 1.

Unlike the existing firewall, a SOAP Firewall filters XML type SOAP messages, on which access control service is provided. Therefore, a SOAP Firewall SHOULD be able to decode and understand XML body contents of SOAP messages that are sent or received.

- ● WS-SProfile 3

WS-SProfile 3 provides Single-Sign-On mechanism using the security token that contains the WS-SProfile 2 security factor.

The mechanism to provide Single-Sign-On means the auxiliary technology to exchange security information: user authentication, approval and property information. On Single-Sign-On camp, there are SAML, Liberty Alliance, .Net Passport, WS-Federation and etc. SAML and Liberty Alliance have worked for the technology to exchange XML-based authentication information, Assertion, while .Net Passport provides Single-Sign-On function through the centralized authentication system. WS-Federation controls federated ID by combining with ID (identity) to represent individual identity, providing the Single-Sign-On function.

- ● WS-SProfile 4

WS-SProfile 4 contains the WS-SProfile 3 security factors, and provides a privacy protection mechanism.

Thus far, the representative privacy protection mechanism is WS-Privacy, which describes a model for a service provider and a consumer to dictate each privacy execution context. In general, it functions as, based on WS-Security technology, the foundation to construct a safe Web services interoperable with new partner (department) with WS-Policy technology and WS-Trust technology. For reference, WS-Policy is a Web service end point policy technology to express and deliver security, credit, transaction, privacy protection, while WS-Trust is a new model that provides an interface, available for inspecting the issuance, exchange and effectiveness of security token.

The following <Table 7-2> shows security factors included in Web service security profiles. (Op) means the availability of each security profile.

<Table 7-2> Security factor by security profiles

Security Factors	**SP 0**	**SP 1**	**SP 2**	**SP 3**	**SP 4**
Transport level data confidentiality	✔	✔(Op)	✔(Op)	✔(Op)	✔(Op)
Transport level data integrity	✔	✔(Op)	✔(Op)	✔(Op)	✔(Op)
Transport level user authentication	✔	✔(Op)	✔(Op)	✔(Op)	✔(Op)
Transport level access control	✔	✔(Op)	✔(Op)	✔(Op)	✔(Op)
Transport level accessibility	✔	✔(Op)	✔(Op)	✔(Op)	✔(Op)
Transport level audit trail	✔	✔(Op)	✔(Op)	✔(Op)	✔(Op)
Message level data confidentiality		✔	✔	✔	✔
Message level data integrity		✔	✔	✔	✔
Message level user authentication		✔	✔	✔	✔
Message level non-repudiation		✔	✔	✔	✔
Message level audit trail		✔	✔	✔	✔
Message level access control			✔	✔	✔
Message level accessibility			✔	✔	✔
Single-sign-on				✔	✔
Message level privacy protection					✔

9.3 Quality Contracts

- ● Development Quality Contract

Security quality is described as a profile in BLA for a security level to be provided when a Web service is implemented. In addition, it inspects whether a desirable level security function operates by tests when a Web service is actually implemented.

● "Web services Use" Quality Contract

When an implemented service is registered to UDDI, what level of security is provided is clarified and whether the security function actually operates should be confirmed by test cases. SLA specifications related to the security quality should specify a method to check whether the specified security level quality is provided, compensation policy in case such a quality fails to be provided and post-management actions in a contract.

9.4 Quality Associates

Major concerns of each associate relating to security quality are summarized as follows.

- ● Stakeholder

A stakeholder analyzes threats related to Web services, determines the required security services to reduce or protect such threats and selects security profile types according to these determinations. The security level is set by the selected security profile and specified in the BLA. In addition, a BLA should contain the range of achievable quality level and the measurement methods. The primary concerns of a Web service stakeholder are determining which security quality level to reduce, to prevent threats and to follow the methods as specified in the BLA.

- ● Developer

A service developer's job is to determine which mechanism is to be used to achieve the security level quality specified in the BLA. Then, a developer is concerned about how to consider the security when developing a service and how to plan tests in order to confirm whether a developed Web service provides a desirable quality level. After all, a service developer is mainly concerned about creating a Web service to secure the security level quality specified in a BLA.

● Provider

A provider is interested if the security quality level specified in BLA can satisfy a consumer

- ● Consumer

A service consumer should comprehend the security level information that is practically required considering the defined security policy and search a Web service to provide the security level information. A consumer also reviews the security policy specified in a searched Web service, acquires an appropriate security token after checking what kind of security token or security claim is required and calls a Web service including the above-mentioned security token suitable for a Web service provider's security policy. Meanwhile, a consumer, as a service requester, may be notified of the results of whether a specified security quality is provided.

● QoS Broker

A QoS Broker performs the security quality test to check the authentication and the quality level inspected by the provider at the time of registration. When a consumer requests certain level of security, the desired Web Services security service is recommended based on the test result.

● Quality Assurer

A quality assurer peforms the quality assurances including Web Services security authentication while monitoring the security quality level between the provider and the user.

- ● Quality Manager

A Web service quality manager is concerned about the management of monitoring and analyzing whether or not the security quality specified in the SLA is provided. In addition, a manager is interested in a system that can analyze the reasons why a security quality is not provided and modify/correct it.

9.5 Related Standards

- ● W3C XML Encryption: XML Encryption Standard. URL: http://www.w3c.org/Encryption/2001
- ● W3C XML Digital Signature: XML Digital Signature Standard

URL: http://www.w3c.org/Signature

- ● OASIS SAML: Standard for interoperation among various security service systems

URL: http://www.oasis-open.org/home/index.php

- ● OASIS XACML: XML-based open standard, SAML is the standard to express security policy

URL: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

- ● OASIS WS-Security Specification: common mechanism standard when security token and message are combined.

URL: http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf

- ● W3C XKMS (XML Key Management Specification): Key management service standard which makes easier to integrate PKI and XML application

URL: http://www.w3c.org/2001/XKMS/

- ● MS, VeriSign, IBM WS-SecurityPolicy (Web Services Security Policy Language): Standard to provide the security policy applied on WS-Security

URL: ftp://www6.software.ibm.com/software/developer/library/ws-secpol.pdf

- ● Ms, VeriSign, IBM WS-Trust: Standard for issuing and exchanging of security token, and trust relationship configuration within various trusted domain

URL: ftp://www6.software.ibm.com/software/developer/library/ws-trust.pdf

- ● Ms, VeriSign, IBM WS-Federation (Web Services Federation Language): The definition of mechanism that makes possible to mediate the user information, property, authentication of Web Services applications which belongs to heterogeneous trusted domain.

URL: ftp://www6.software.ibm.com/software/developer/library/ws-fed.pdf