2012 3rd International Conference on e-Education, e-Business, e-Management and e-Learning
IPEDR vol.27 (2012) © (2012) IACSIT Press, Singapore

Cooperating the web services as distributed to create a Non-Repudiation service

Mohammad rostami[1], Esmaeil bagheri[2] and Maryam lotfi[2]

[1] Member of Young Researchers Club, Islamic Azad University, Dehaghan Branch, Isfahan,Iran
[2]Department of Computer, Islamic Azad University, Dehaghan Branch, Isfahan,Iran

Abstract. Web services enable desktop and web applications to access functions in them with communication on HTTP and to receive its conclusion in the standard format platform of XML. Web services don't depend on programming language, platform and special protocol. It means that you can use of Web services with each programming language on each platform. One great example of standardization in an enterprise today is web service.Web services expose functionality that can be discovered and consumed in a technology-neutral, standardized format. A web service is just one kind of implementation of a service. Web services are just a catalyst for an SOA implementation.A Web service sends the result of its processing to applicator program in XML format platform by HTPP. XML format is a standard way for communicating between two adverse systems. Web services messages are sent by using of HTPP because of easily receiving to applicator on network and without blocking by fire walls.
Web service is a software which provides accessibility to data and also data processing systems independent of different hardware and software platforms by using of standard protocols of exchanging net data. Web services exchange data as distributed or interoperate with each other to perform a work. To interoperate with these web services, it should be made a protocol between them to able cooperate together in addition of preserving security. For this purpose, it can be used of WS-Trust protocol that describes a model to make direct and indirect trust communications with interface. WS-Trust defines junctures for WS-Security.That non repudiation service can be established by the Protocol Tsp(time stamp protocol).This service is part Pki(public key infrastructure).

Key Words： Web service, distributed system, non repudiation service,TRUST,TSP,PKI

1. Introduction

Web services are new technologies that provide interaction between machine to machine on a network by using of a set of standardized technologies consists of WSDL, SOAP, and UDDI [2]. Under these technologies, UDDI is designed to find the services that provides an access to WSDL documents and it includes four core types of information: business Entity, business Service, binding Template, t Model [6]. Web services may use of other web services to perform their works.In simple word, it can be said that web service is a traditional web service (like nominating service, weather report service producing electronic and etc) that is available by network [5]. Web service follows of a set of standards that is caused service-consumers who follow of them to obtain them by network. These standards make the architecture core of web component [14]. A web service is not an object model and is not protocol specific. In other words, it's based on a ubiquitous web protocol (HTTP) and data format (XML). A web service is also not dependent on a specific programming language [8].You can choose to use any language or platform as long as you can consume and create messages for the web service [5].

[1] + Corresponding author. Tel.: + (989132893902).
E-mail address: (mohamad.rostami10@yahoo.com).
[2] bagheri471@gmail.com
[3] lotfi.sh@gmail.com

In this paper, it is explained that, the web services can be interoperated as distributed for create non repudiation service [1][12].

2. Surveying on Web Service Standards

One great example of standardization in an enterprise today is web service. Web services expose functionality that can be discovered and consumed in a technology-neutral, standardized format[15]. A web service is just one kind of implementation of a service. Web services are just a catalyst for an SOA implementation. One of the definitions that is accepted by some is as follows: "A web service is a programmable application component accessible via standard web protocols." The key aspects of a web service are as follows[16]:

Standard protocol: Functionality is exposed via interfaces using one of the few standard Internet protocols such as HTTP, SMTP, FTP, and so on. In most cases, this protocol is HTTP.

Service description:Web services need to describe their interfaces in detail so that a client knows how to "consume" the functionality provided by the service. This description is usually provided via an XML document called a WSDL document. (WSDL stands for Web Services Description Language.)

Finding services: Users need to know what web services exist and where to find them so the clients can bind to them and use the functionality. One way for users to know what services exist is to connect to a "yellow pages" listing of services. These yellow pages are implemented via Universal Discovery, Description, and Integration (UDDI) repositories (These can be private or public UDDI nodes.) [15][16].

XML (Extensible Markup Language): XML is a markup language that provides a format to describe data. Like html, it consists of tags, etc. XML was provided as structured self-describing method to represent data that is totally independent of application, protocol, terms, operating system or even programming language. Many nominate XML as language mixed with other business languages, because it is widely used by all companies to transport loadable business data[2].

SOAP (Simple Object Access Protocol): soap is a lightweight communication protocol for web services based on XML. It is used to exchange structured and typed information between systems. SOAP allows you to invoke methods on remote machines without knowing specific details of the platform or software running on those machines. XML is used to represent the data, while the data is structured according to the SOAP schema. The only thing both the consumer and provider need to agree on is this common schema defined by SOAP. Overall, **SOAP keeps things as simple as possible and provides minimum functionality[5].

WSDL (Web Services Define Language): wsdl (pronounced as "whiz-dull") forms the basis of web services and is the format that describes web services. WSDL describes the public interface of a web service including metadata such as protocol bindings, message formats, and so on. A client wanting to connect to a web service can read the WSDL to determine what contracts are available on the web service. WSDL is similar to Interface Description Language (IDL) for web services. The information from the WSDL document is typically interpreted at design time to generate a proxy object. The client uses the proxy object at runtime to send and receive SOAP messages to and from the service.

IDL is a standardized language used to describe the interface to a component or routine. IDL is especially useful when calling components on another machine via RPC, which may be running on a different platform or build using a different language and might not share the same "call semantics."

A WSDL document has three parts, namely, definitions, operations, and service bindings[4][14].

UDDI (Universal Discover Description Integration): uddi is a platform-independent directory protocol for describing services and discovering and integrating business services via the Internet. UDDI is also based on industry-standard protocols such as HTTP, XML, SOAP, and so on, and it describes the details of the services using WSDL and communicates via SOAP. The philosophy behind UDDI is like a traditional "yellow pages" where you can search for a company, search for the services its offers, and even contact the company for more information.A UDDI entry is nothing but an XML file that details the business and the services it Offers[10][14].

3. Web Services Interoperate as Distributed

Web services exchange data as distributed or interoperate with each other to perform a work. To interoperate with these web services, it should be made a protocol between them to able cooperate together in addition of preserving security. For this purpose, it can be used of WS-Trust protocol that describes a model to make direct and indirect trust communications with interface[17][11]**.** WS-Trust defines junctures for WS-Security that provides the following cases:

- The methods for distributing and exchanging security tokens
- The methods to configuration and access to the trust communications

Similar to SAML, the WS-Trust defines a request/response mechanism to obtain security token[17].

The web service security model defended in WS-Trust based on a procedure which is necessary for a web service to confirm a set of request by an entry message.(for example name, key, credit, ability and etc). If a message entered without having needed document for requests, the service will ignore or reject whole message. A service can point to needed requests and related data on its policy that has been described by WS-Policy and WS-Policy Attachment. A request agent can send those messages which show its ability to confirm in the set of its needed requests by depending security token on messages and placing messages signatures which represent possessing document of tokens. A short definition of WS-Trust model is that a web service has an applied policy on it, it receives a message from an applicator that may consist of security tokens and may have a number of applied security or safety on it by using of WS-Security mechanisms[1]-[12].

The most important WS-Trust specifications are as below

- The communication between web service applicator, web service provider and security token service (STS)**.** -Both Request Security Token and Request Security Token Response models. security token services form the fundamental of trust by publishing security tokens which are able to use for interface trust communications among different certificated domains[3][17].

4. Non-Repudiation

Non-Repudiation is a guarantee that anyone can't repudiate a thing. Generally, Non-Repudiation is ability to confidence of that, a class of obverse contacted with; it can't reject the validation of its signature on a document or send a message resulted from it[13]. For many years, the authors have searched for impossible repudiation on some locations. For example, you may send a registered mail, thus the receiver can't repudiate to deliver the mail. Non-Repudiation is a known concept in Engineering field, which provides measures that, contributors on a communicating process aren't able to repudiate their presence. This concept has a significant importance in business fields based on the architecture of realism service. (As an example, Issuing electronic account).A framework to present Non-Repudiation in creating service by cooperating web services as distributed, it can be introduced TSP protocol[18].

5. Cooperating the web services as distributed to create a Non-Repudiation service

By Cooperating web services as distributed, it can be created Non-Repudiation service by TSP protocol that, the service is considered a part of PKI[19]. TSP is a main security component on the electronic world, and PKI is a set of solutions for the problems related to secure distribution and cases such making trust between the persons. Public Key Infrastructure supports basic security mechanisms such as confidentiality, Integrity, Authentication and Non-Repudiation. In fact, PKI is a spine that the other programs and security parts are made on it[9].

Four main services, which provided by PKI specially, are[9][11]:

- Confidentiality
- Integrity
- Non-Repudiation
- Authentication

Understanding of this point has much importance that PKI is only no one of the fourfold mechanisms of confidentiality, Authentication, Integrity and Non-Repudiation, but it is a framework that supports these mechanisms and services.

Confidentiality: Confidentiality means that, it could be guaranteed data confidentiality by using of standard protocols and infrastructure mechanisms.

Integrity: Integrity means that data can't change or be destroyed, and also interactions can't be freed as half-finished.

Authentication: Authentication means, to revision and control the ID of existence by testimonies of Public Key and digital signatures. Authentication is well Performable on the electronic commerce world by Public Key Infrastructure Systems considered in PKI structure.

Non-Repudiation: It means that credit data will not be rejected in the future or a performed interaction can't be denied in the future. Non-Repudiation is considered very important service on electronic, commerce and financial exchanges and legal subjects[7].

Four main functions that are implemented by all PKIs and considered as a kind of common functions, including:

- Public Key Infrastructure: including the problems related to creation, distribution, management and control of keys.
- Issuing certificate: A function which conditions a Public Key to a special organ, a real person or any other existence, or to a data party. As an example, an Email or an order of buy.
- Credit verification certificate: to revision and control the subject that, a secure and reliable communication is formed and the certificate is still valid for a special function[9].

To cancel certificate: to cancel and phase out under issued certificate and send this issue to the public by CRL mechanisms to OCSP. The issue of PKI has many complications and it is developing and optimizing daily for the activities that set in the field of electronic commerce. Although, available technologies greatly response to the current necessities, but it is still debated much issues in the field of interaction ability and also productivity of this system. Despite, PKI has presented numeric beneficial cases to solve special security necessities[7][19].

6. Conclusions

Web service is a software which provides availability to data and also processing data systems as distributed regardless of different hardware and software platforms by using of standard protocols of Internet data exchange. In simple explanation, web service is a component of an available application by standard communicating protocols. Web services as distributed, exchange some data or cooperate together to implement an action. By cooperating web services, it can be created a Non-Repudiation service by TSP protocol that, the service is considered as a part of PKI. The framework of a PKI contains security and functional policies, security services and protocols that applied by using of Public Key Infrastructure to manage the keys and testimonies.

The goal of PKI is to create a secure and reliable bed for secure data exchange, financial documents, money and etc in an environment that isn't secure in nature such Internet. In fact, it could be took a hierarchy of trust by PKI. The concept of trust in PKI is greatly related to CA. In the environment of network, different existences that are communicated together, they aren't identified together normally and there is no trust to the others and they need to make a mutual confidence to implement financial and commercial interactions. In fact, the implementation of a PKI provides the mutual confidence by using of a CA(certificate authority).

7. References

[1] hoops.Web Services as Distributed Systems.Part 1, December 7, 2010.

[2] Richard Monson;*Haefel.Web Services: XML SOAP WSDL UDDI WS-I JAX-RPC JAXR SAAJ JAXP* .

[3] M.Tamer Ozsu ,P . Valduriez . Principles *of Distributed Database System* . Prentice Hall , USA , 1999.

[4] Christensen E.,et al,"*Web Services Description lanquage(WSDL)1. 1*" ,http://www.w3.orgITR/2001/NOTE-wsdl-20010315,March 2001.

[5] Ethan Cerami. *Web Services Essentials* , February 2002.

[6] Ehnebuske D.,et al,"*UDDI Version 2.04 API*",http://uddi.org/pubs/programmersAPI_V2.04-published-20020719.htm,july 2002.

[7] Tom Austin,*PKI-A Wiley Tech Brief,Wiley*,John & Sons Incorporated,2000.

[8] chase,Nicholas, *understanding Web Services Specifications*. Aug 2006.

[9] Peter Gutmann,*Everything you Never Wanted to Know about PKI but were Forced to Find Out*,University of Auckland,2005.

[10] Ehnebuske D.,et al,"*UDDI Version 2.03 Data structure* Reference",http://uddi.org/lubs/Datastructure_V2.03 Published-20020719.htm ,july 2002.

[11] Bertino ,Elisa, Martino ,Lorenzo, Paci ,Federica, Squicciarini ,Anna. *Security for Web Services and Service-Oriented Architectures*. Springer, 2009.

[12] O'Neill ,Mark . *Web services security*. McGraw-Hill Professional, 2003.

[13] Toshihiko Matsuo and Shin'ichiro Matsuo,*on Universal Composable Security of Time-Stamping Protocols*,NTT DATA Corporation,2005.

[14] Periorellis ,Panos . *Securing Web services: practical usage of standards and specifications*. IGI Global snippet, 2008.

[15] Papazoglou ,M. *Web services: principles and technology*. Pearson Prentice Hall, 2008.

[16] Zhang ,Liang-Jie, Jeckle , Mario. *Web services: European conference*, ECOWS 2004, Erfurt, Germany, September 27-30, 30, 2004.

[17] Birman ,Kenneth Paul . *Reliable Distributed Systems: Technologies, Web Services, and Applications*. Springer, 2005.

[18] C.Adams,*Internet X.509 Public Key Infrastructure Time-Stamping Protocol (TSP)*,RFC 3161,2001.

[19] NIST PKI Project Team,*Certificate Issuing and Management Components Protection Profile*,2001.