

# Security Accessing Model for Web Service based Geo-spatial Data Sharing Application

Guoqing Li<sup>1</sup>, Chenhui Li<sup>1,2</sup>, Wenyang Yu<sup>1</sup> and Jibo Xie<sup>1</sup>

<sup>1</sup>(Key Laboratory of Digital Earth, Center for Earth Observation and Digital Earth, Chinese Academy of Sciences, Beijing 100086)

<sup>2</sup>(Graduate University of Chinese Academy of Sciences, Beijing 100080)

**Abstract:** Web service and its related service oriented architecture (SOA) have brought new infrastructure for geo-spatial data sharing. However, the lack of uniform security mechanism for service-based geo-spatial data sharing applications has blocked its usage in many operational applications. Taking multi-agency Earth Observation (EO) data collaborated accessing as example, this paper studied the basic requirement of service based EO data platform, and presented a collaborative security accessing model. Because there are four user types and five operations were identified, four levels security control are proposed as portal level, service level, database level and network transmission level. Each data request from end-user will be operated and go through all four levels before collecting the result from certain data resource. Based on the different existent security mechanisms for above levels, a collaborative security accessing model was studied to keep the Single-Trust for each kind of user. Accessing right level was used to evaluate the access classification in different database and uniform it to be standard classification. As a result, the portal user with certain access right can only get the right-matched EO data from different CA covered data resource in this platform. The proposed security model in this paper can bring one feasible securely accessing method to distributed geo-spatial data resources.

**Key words:** security mechanism, data sharing, accessing model, WS-Security, CA

## I Introduction

The rapid worldwide deployment of the Internet and Web is the enables for a new generation of geo-spatial data sharing application, which based on the web service, but the provision of a security architecture that can ensure the privacy and security of geo-spatial data sharing is still an open question.

In the field of earth observation, geospatial data sources are always geographically distributed stored. And these data sources belong to different social organizations and institutions, their management and storage methods are not exactly the same. For some organizations, due to data security needs, data will also be distributable stored. Therefore it is very important to build up the geospatial data sharing infrastructure to realize geospatial data sharing. Spatial data sharing technology based on the web service or OGC Specification has made considerable progress. However, the lack of uniform security mechanism for service-based geospatial data sharing applications has affected its usage in many operational applications. For example, data services based on OGC specifications has not yet set up a unified security framework to ensure the security access to services [2]. Some operating data sharing system simply uses the static password authentication method to verify user identity, which is lack of a unified security solution. Because of these defects, most of the existing data sharing system can not feed the high security demand of some application scenarios. Especially in the complex cross-cutting applications, Often need to involve many different agencies and resources, these resources are integrated into a virtual organization temporary, in which data resources are needed to be re-arranged and

defined the role. But these organizations and resources have different security attributes and security requirements. How to build a unified security mechanism to meet this need is particularly urgently needed [10].

Computer network security provides a lot of security technologies for the secure sharing of spatial data, such as data transmission technology security, authentication and digital signature technology. However, spatial data sharing in the current system is less practical use of these security mechanisms. Even lack of a unified security model which full use of these technologies to protect the security of distributed spatial data sharing.

In this paper, with the actual needs, build up a security platform for multi-agency Earth Observations data sharing and cooperation. Try to establish a unified security framework to meet the needs of multi-organization, multi-user type, multi-security level, and distributed geospatial data sharing applications.

## 2 Multi-agency Data Sharing Security Challenges

### 2.1 Multi-user, different permissions, different functional

In the multi-source geo-spatial data sharing applications, often require different organizations and institutions of different types of spatial data sharing and security management and makes these organizations and agencies work together to achieve and improve the efficient use of data resources and scope. Therefore need to divide different organizations and resources into many virtual temporary organizations, these resources will be re-arranged, and define its role in the application scenarios. So in the spatial data sharing application, there usually have several types of users, multiple permission levels and many different operations behavior of the resources, these are bringing difficulties for the system security mechanisms design. In the common multi-source spatial data sharing application there are four main types of users as following [3]:

- 1) Application Users or Portal Users
- 2) Resource providers
- 3) Node resource management users
- 4) Data sharing system administrator

These users have five operation behaviors to the resources:

- 1) query and access the resources
- 2) Resources publishing
- 3) Resources management
- 4) Resources collection
- 5) Resource application

*Table1. User type and behavior Analysis*

User Type	User roles	Description	User behavior
Portal users (end users)	1) query data, download or do other operations through the Portal	the end user of the data resource	1、 5
Resource providers	1) Use the system tools to upload, remove and classification the data that shared	Resource providers is the owner of the data resource	1、 2、 5
Node resource manager	1) configure and maintain the virtual data node 2) classify and authority the node users	Node Manager specified by the resource providers	1、 3、 5

Data sharing system administrator	1) authentication and authorization the resources providers 2) authentication portal user and user type examination 3) maintain the operation of Portal	Data sharing system administrator	1, 3, 4, 5
-----------------------------------	---	-----------------------------------	------------

In the data sharing system, different types of users have different behavior and roles, should have different permissions. Although the same types of users, should have different access right to different data resource in the collaborative data sharing system. Native node resource Manager can authorize users that use the data resources within the organization and modify the user's permission level in the organization.

## 2.2 Security Requirements of geo-spatial Data Sharing System

In multi-source geo-spatial data sharing applications, the system needs from the data transport layer security, database security, data services security and the data portal security these four levels to analysis and design the system security model, and use the appropriate security mechanisms to meet the needs of different types of users. In the geo-spatial data sharing system, specified requirements are as follows [1]:

- 1) Single-Trust sign-on
- 2) User authentication and identification
- 3) User Permissions classification
- 4) Data Resource Classification Management
- 5) Uniform credentials/certification infrastructure
- 6) Support for security invoke of service
- 7) Data transmission Security
- 8) Interoperability with local security solutions

When different users log in through the portal, should first check their identification and authentication, then confirm the user's permission level. When the user invokes the data service, only return the data set within the user's access right, and the requested data should be delivered to end-users through the secure transmission channel. Geo-spatial Data sharing system should provide the capability that each data resource provider and manager can easily authorize the end-users, and classify different data into different security level.

## 2.3 Multi-level security issues

In the data sharing system, not only have different user types, different permissions and other issues, while facing multiple levels of security, including data transport layer security, database security, data services security and the data portal security. Sensitive data cannot be transmitted in plain text form and encryption protocol for transmission should be used.

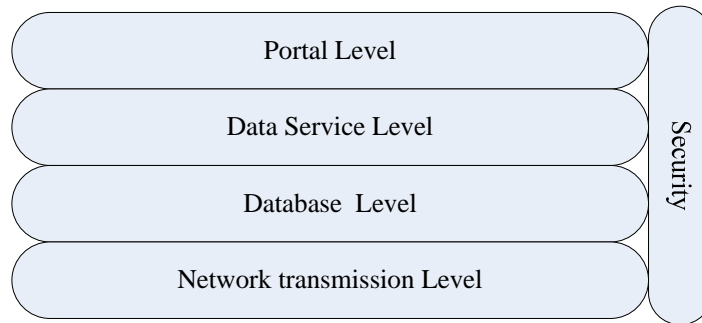
End users with different security level can access different data sets, how to manage user permissions, how to manage and classify the data resources, all these are challenges.

Service-based geo-spatial data sharing in the current model are the lack of uniform security mechanism, which gives the application of service-based geo-spatial data sharing system a great challenge.

## 3 Collaborative Security Accessing Model

In our data sharing system, the entire system is divided into four components: 1) data sharing portal, 2) data

resource virtual nodes, 3) directory service centers, 4) service registration management center and the CA center. Collaborative Security framework consists of four levels: data-sharing portal security, data services security, data resources security and data transport security, we design the system from all four levels.



*Figure 1. Security in different Level*

In our collaborative security accessing model, we integrate a variety of existing security mechanisms and modify them to meet the new requirements. In the model, the certification authority mechanism is used. One unique CA center is setup for our application and used to sign the digital certificates to the portal users and services. Portal users use the digital certificates to be authenticated and log in the portal, and use a variety of services such as data query, data acquisition, etc. System Services client and server also needs to be authenticated through digital certificates.

In order to manage the users and data resources more reasonable, we bring in access control mechanism and establish the different access authority and the security level for system's application user and the data resources. When user's access authority is higher than the security rank of the data, then the user may retrieve the data and carry on downloading. When user's access authority is lower than the security level of the data, this user can only retrieve this data, cannot download it. The user has the different jurisdiction rank in the different organization, may download and use the data resource in different organizations with various security levels [6].

In the data transmission level, we use the https protocol to transport the data safely. During transmission, all data are encrypted. The sensitive data cannot be decrypted even if they are eavesdropping, which gives the Earth observation data strictly protection.

System's data downloading uses SIG protocol which based on the FTPS protocol. When the user inquired the data they need through the portal, the special-purpose safe downloading tool must be used.

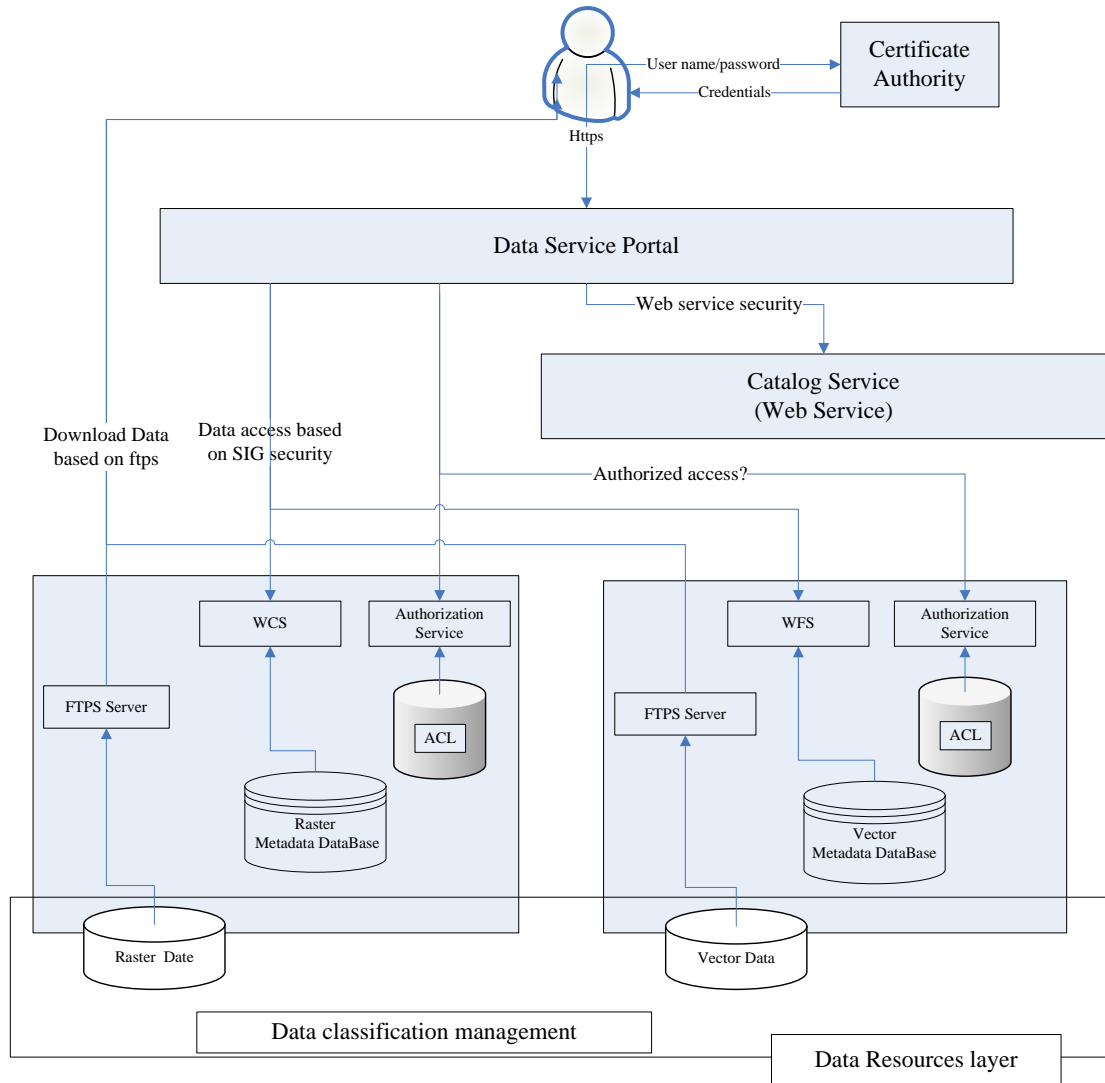


Figure 2. Collaborative Security System Architecture

## 4 Security Model Implementation

### 4.1 Security authentication mechanism

In the portal layer, confirmation and the recognition of the user's identity are needed. The identification authentication and the recognition commonly use safety mechanism like the traditional static password authentication technology, the CA certificate authentication technology and so on. The static password authentication is used the user's name and the password to confirm the user' identification .Identification authentication in this way is a simple and safety mechanism that is easiest to implement, but the security is low, in many cases, because of the risk of password leakage. So CA certificate the authentication is considered for the high security multiple sources geospatial data sharing application.

#### 4.1.1 CA certificate mechanism

A CA issues digital certificates that contain a public key and the identity of the owner. The matching private key is not similarly made available publicly, but kept secret by the end user who generated the key pair. The certificate is also an attestation by the CA that the public key contained in the certificate belongs to the person, organization, server or other entity noted in the certificate. A CA's obligation in such schemes is to verify an applicant's credentials, so that

users and relying parties can trust the information in the CA's certificates [7].

#### 4.1.2 Authenticate System Implementation

Data sharing system establishes a unique root CA as CA center, data sharing system administrators responsible for maintaining. When a new application user wants to join the system need to be registered to the CA center, fill in user information, and then after reviewed by CA center, will get the user's digital certificate issued by CA center. Data resource management user who setup and manage the virtual data node also have to apply for the server certificate when deploy the data services in the virtual node.

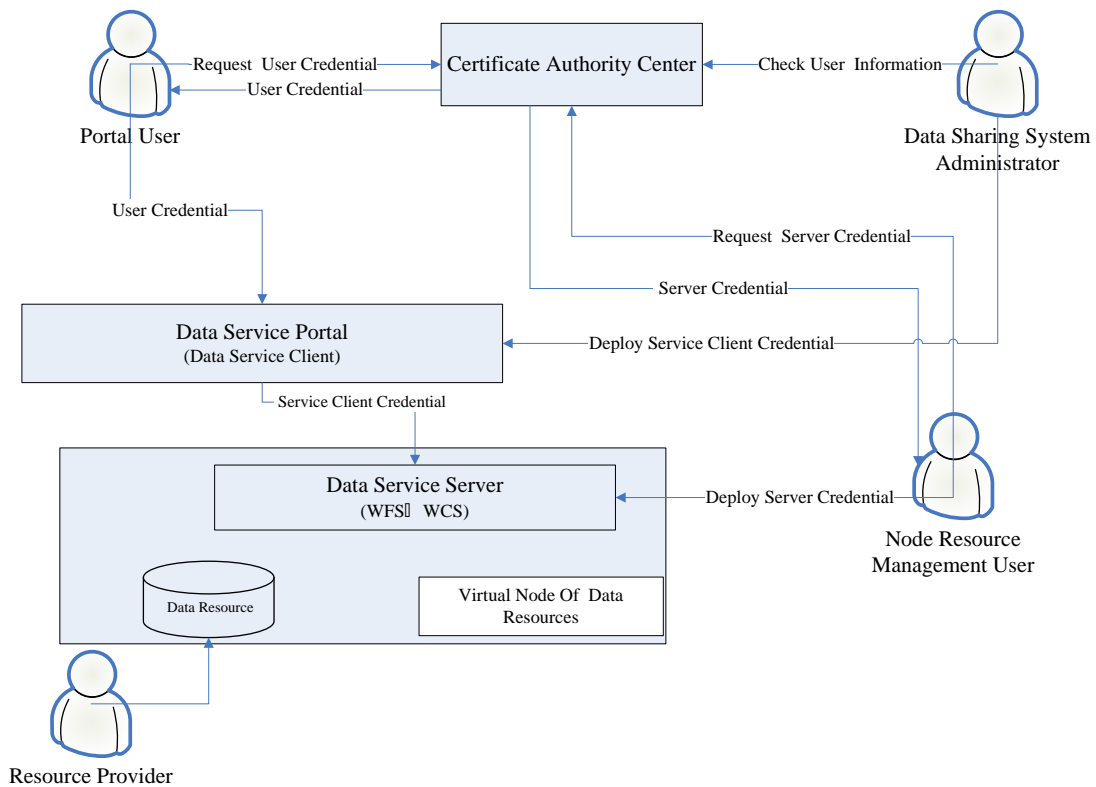


Figure 3. Authenticate system structure

#### 4.2 Access Control Mechanism

Any computer system has two resources: active subject and passive objects. In database systems, users, processes, etc. is the active subject; the object is the data, tables, records, fields, etc. Access control is needed when the active subject request to visit the passive object. System need to check the rules according to the subject of the user and group identifier, the security level and privileges, the object of the security level, access rights, and then decide whether allow active subject to access the requested passive object[11].

Access control is divided into DAC (Discretionary Access Control) , MAC(Mandatory Access Control) and RBAC (Role-Based Access Control) three types. Considering the need of the data sharing application about data security and the need for multi-user access control, we use the improved MAC model that is Multi-Level Security [14].

MAC is mandatory access control model, system users and resources are given a certain level of security, control of the Execute Access, the system first visit to the principal and resources on the security level of comparison and decide whether to visit the main access to the resource. Model gives the system security level for each user a unique

label.

In spatial data sharing system, due to multiple data provider organizations, each data resource providers can classify the data resource they provide into level 0-9. Each portal user in different organizations has different permission levels for 0-9 grade level. Each user can only access the documents and data under his permission level, he cannot access the data has the security level higher than his permission level.

In the virtual data node, the data node administrator is responsible for the management of the node resources, and responsible for data classification. The node administrator will put the data with lowest security rank into directory 0, and put in the higher security rank data into the higher security directory. Simultaneously the data node administration user also needed to already the application user assignment corresponding access authority which registered in the data sharing system, the new registration's application user's default access authority was 0 levels. When inquires using the user through portal oneself are interested the data, the portal user jurisdiction control module (authorization engine) traversal each data dummy node, inquires this user's permission rank in each organization through ACL (access control list) [14].

### **4.3 Data Services Security Mechanism**

When the portal user through the portal to check the data they need, the data portal client will invoke WFS or WCS service in the node where the data is storing. Then how to ensure the security of data services is the next step. As the standard WFC, WCS services have not improved the security framework, we use the standard web service security mechanisms to ensure the security of data services accessing. WS-security is a very reliable and flexible security mechanism. WS-security has the following advantages [4]:

- 1) Compared with the SSL which can only provide point to point security, WS-security can provide end to end security;
- 2) WS-security provision of the security token (X.509 certificate or Kerberos, etc.) and information associate general mechanism;
- 3) Ws-security could combine with existing security protocols and encryption technology to build a flexible security model based on the actual security requirements;

According to the need of multi-agency Earth Observation (EO) data collaborated accessing, we have established SIG security solution which based on the WS-Security and digital certificates. SIG security solution uses the public key technology and X.509 digital certificates. The client and server both have their own X.509 digital certificates which signed by the unique CA center [7].

SIG-Security solution contains two parts, the client side and the server side, when the client call the service, responsible for the use of digitally signed SOAP message [5] and prove the identity of the service initiator. Server deployed in Tomcat-Axis environment, the server side will first verify the identity of the service initiator through the signature of the client SOAP messages, when identity is confirmed, and the server side will carry on the local subscriber status mapping. Therefore the service end is composed of two parts: Based on digital certificates' user status authentication and the local subscriber status mapping [24].

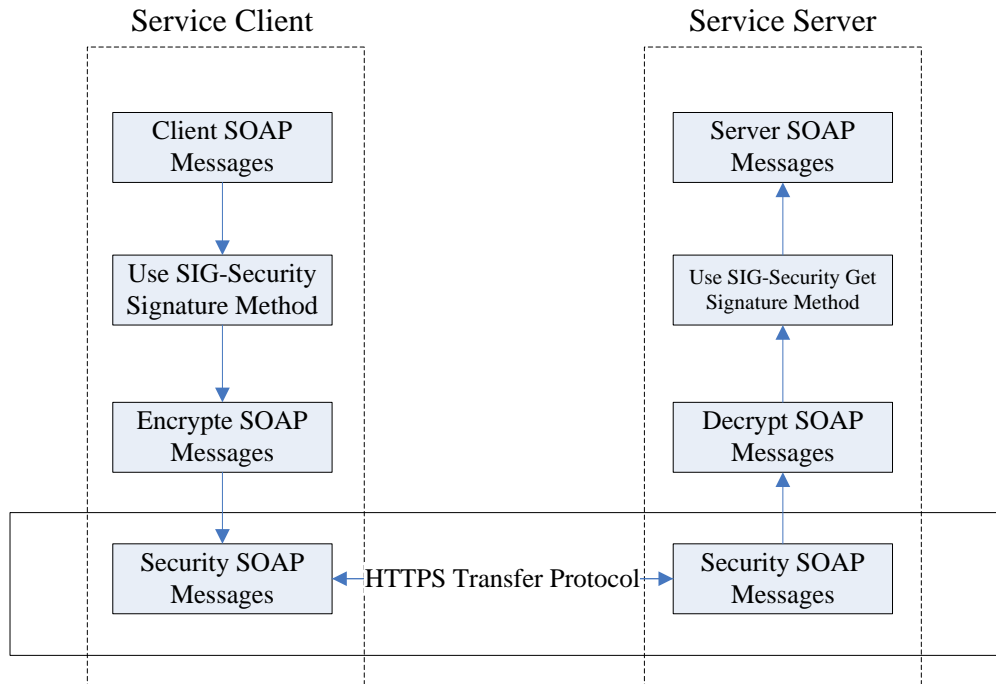


Figure 4. Web service security illustration

#### 4.4 Data Transport Layer Security

In spatial data sharing systems, data transport security mechanism is in the lowest level of security system. However data transport security is the most basic and most important security mechanism. It is the basis for other security measures and security technology. If there is no data transmission layer security, all the security mechanisms are the castles in the air. The security of the data transport layer is divided into two parts [20]:

- 1) Communications security of client requests and server response;
- 2) Sensitive data secure transmission when application users want to download data.

In order to protect the client and server communications, we use https protocol to protect the security of the communication process based on CA certificates. Https (hypertext transfer protocol over secure socket layer), is a security-oriented http channel. It uses a different port compare with the default http port and have a layer of encryption and authentication, which is between http and TCP. Https protocol's security infrastructure is SSL, which is to add SSL on http transport layer.

This transfer protocol was originally developed by Netscape, provides identification authentication and encrypted communications method, and now it is widely used in the World Wide Web security-sensitive communication. Use the https protocol can provide the following security [21]:

- 1) authenticate users and servers, to ensure that the data is sent to the correct client and the correct server;
- 2) Encrypt data to prevent data from being intercepted;
- 3) Maintain data integrity, ensure data is not altered during transmission.

Data Services based on web service, currently most of the web service implementations are based on http as its transport protocol, and it can be a good use of https protocol with web service security mechanisms, making the system provides a variety of security mechanisms work together.

In order to download the data securely, we provide SIG protocol to safely download the data, using specially developed SIG download tool. SIG download tool supports download based on security transmission protocol FTPS. SIG download tool automatically binds the browser, when portal user download the data, the browser will immediately boot up the SIG special download tool. SIG tool supports resume broken transfer and multi-task mechanism.

## 5 Conclusions

This article analyzes the security requirements of multi-agency Earth Observation data sharing application, combined with many existing security technologies. A security framework and model for multi-agency geospatial data sharing is introduced. In the security model, we have used the foundational security protocols, to ensure the security of the communication and data transmission. And based on these important security protocols, the model established the CA certificate authority mechanism, the access control mechanism as well as the data service security solution, and make these security mechanisms work together to meet the needs of the multi-agency, multi-user type, multi-level permissions in data sharing application. The model classified the users and data resources into different levels, feed the need of personalization and custom-made and implemented the diversified security policy between different Earth Observation organizations.

## 6 Acknowledgements

This work is financial supported by National High Technology Research and Development Program (No. 2008AA121501) and National Basic Research Program of China (No. 2009CB723906).

## 7. References

- [1] Von Welch , Frank Siebenlist, Ian Foster, John Bresnahan Security for Grid Services, High Performance Distributed Computing, 2003.
- [2] <http://www.opengeospatial.org/standards/wps>
- [3] Guoqing Li, Dingsheng Liu, Zhenchun Huang, Yi Zeng, Yong Xue, Spatial data service models in Grid environment, LNCS 4331, p 598-602, Springer Press, 2006.
- [4] JING Jian-du , Research and implementation of WS—Security in Apache Axis 1.1, Computer Engineering and Design, 2005 ,Vol.26 No.7
- [5] Simple Object Access Protocol (SOAP), W3C, 2000.
- [6] Belani,E., VBelani, E., Vahdat, A., Anderson, T. and Dahlin, M. The CRISIS Wide Area Security Architecture. 8th Usenix UNIX Security Symposium, 1998.
- [7] [http://en.wikipedia.org/wiki/Certificate\\_authority](http://en.wikipedia.org/wiki/Certificate_authority)
- [8] IBM, Microsoft and VeriSign. Web Services Security Language (WS-Security), 2002.
- [9] XML Encryption Syntax and Processing, OASIS, December 2002. <http://www.w3.org/TR/xmlenc-core/>
- [10] Ian Foster, Carl Kesselman, Jeffrey M. Nick, Steven Turcke, The Physiology of the Grid: An Open Grid Services Architecture for Distributed Systems Integration.
- [11] Zhu liang gen, Lei zheng jia, Zhang Yu qing, Research of Database Security, Application research of computers, 2004 21(9).
- [12] IBM, Web Services Conceptual Architecture (WSCA1.0) , 2001.
- [13] Matunda Nyanchama, Sylvia L. Osborn, Access Rights Administration in Role-Based Security Systems, IFIP Transactions; Vol. A-60
- [14] SHI Wei-peng, YANG Xiao-hu, SOAP-based Fundamental Security Specification of Web Service(WS-Security), Application

research of computers, 2003, 20(2)

- [15] Guo Wei, Mao Bing , Xie li, Madantoty access control (MAC) design and implementation, Computer Applications and Software, 2004, 3, Vol.21
- [16] WANG Fan, Li Yong, LANG Bao-ping, LI Cheng-xu, Securing SOAP Message Exchange with WS-Security, Computer Applications, 2004,4,Vol.24
- [17] ZHANG Wei-yong, CHENG Jun, WANG Jian-xin, Design of web services security based on WS-Security Specification[J], Journal of HEFEI university of technology, 2006,8,Vol.29
- [18] [http://www.oasis-open.org/committees/tc\\_home.php?wg\\_abbrev=ekmi](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ekmi)
- [19] The Web-o-Trust Project. <http://www.web-o-trust.org/>.
- [20] Open GIS Consortium. About OGC [EB/OL]. 2008. <http://www.ogcnetwork.org>.
- [21] [http://en.wikipedia.org/wiki/HTTP\\_Secure](http://en.wikipedia.org/wiki/HTTP_Secure)
- [22] <http://en.wikipedia.org/wiki/SSL>
- [23] <http://en.wikipedia.org/wiki/WS-Security>
- [24] Scenarios, Patterns, and Implementation Guidance for Web Services Enhancements (WSE) 3.0  
<http://msdn.microsoft.com/en-us/library/aa480545.aspx>
- [25] Zheng Chun Huang, thGrid-Security Tutorial, 2009,5
- [26] WPS 05-007r7\_Web\_Processing\_Service\_WPS\_v1.0.0.pdf
- [27] <http://www.opengeospatial.org/standards/requests/28>
- [28] <http://www.w3.org/>