THE SECURITY MODEL FOR DATA EXCHANGE USING XML ENCRYPTION AND SECURITY TOKEN IN WEB SERVICE

Ari Muzakir*, Usman Ependi[†]
*Bina Darma University
Jl. Ahmad Yani No 12 Palembang
e-mail: ariemuzakir@mail.binadarma.ac.id

[†]Bina Darma University
Jl. Ahmad Yani No 12 Palembang
e-mails: usman@mail.binadarm.ac.id

Keywords: *Data Exchange, web service, xml encryption, username token*

Abstract. *Nowadays, security being the important issue in information and technology era, especially when it use the internet. The web service who has XML technology on their exchange data is implement the use of public-key cryptographic techniques as well as the insertion of username tokens to the authenticity of the sender as a means of securing data. Implementation has been done using the security library will facilitate in building a web service security. XML Encryption that uses RSA algorithm with a key length of 1024 bits is able to provide protection against the transmission of data between the client and the web server to the database service. Username token role in providing the authenticity of the message is to use RSA-SHA1 cryptography. The results obtained are SOAP request message is encrypted and decrypted properly afford and integrity, authenticity, and security of data is maintained.*

1 INTRODUCTION

Nowadays, the importance of security data in data exchange being bolder especially in internet era. The web service is becoming popular in enterprise because of its ability to integrate the applications from different platform using XML document. XML (eXtensible Mark-up Language) is a standard for defining data in simple and flexible form. Even web service support the communication and integration using XML and web, the security factor between the client to the server web service on this communication channel not fully guaranteed. It is proven by the many factors that cause the cracks threats to web services such as was done by previous research.

A message which was sent by the web service is still a XML data, so this led to the possibility of the original data is not received by the recipient. Although the message is encrypted using an algorithm that does not mean that the message received by the recipient really pristine, because it could be that the structure of the message has been changed when a message is sent or when it is received.

For web service security issues, in previous cases, most of the research conducted in only one model of security or safety standards on a single web service only. So in these cases, the security system still perceived less in providing a maximum protection against security

threats web service, both for the client to the server service and vice versa. Although in general, the condition is considered to have been able to meet safety standards. The constraints encountered when discussing about the web service is still some doubt as to implement the web service. Especially to those who use the Internet on their transactions. These uncertainties arise from the security level of web service technology itself. Security aspects become very important to keep that data or information is not misused or accessed arbitrarily [1]. WS-Security also arranges how to insert security tokens in SOAP messages in plaintext form or in binary form, such as X.509 certificates [3].Therefore, this study will try to present a model of prototype security in the exchange of data on the web service. Using means to encrypt and insert a security token in the SOAP request and response message using XML Encryption.

2. LITERATURE REVIEW

Some researchers have been conducted regarding the web service's security, such as the specification of web services security specifications and how to deal with threats to the security of web services. Several studies also have focused on web security service which is still immature such as CORBA and RMI [3].

Furthermore, on how to address the challenges in Web services security is to present an integrated security framework or framework based on use of authentication, authorization, confidentiality, and integrity mechanisms on the web service. Framework serves to integrate and implement these security mechanisms in order to attack a powerful web service [2]. Previous research also discusses the presentation of a comprehensive method for a guarantee of security services in SOA, where the proposed method defines three stages of security analysis, security architecture and the identification of WS-Security standard [4].

In addition, research on web security service has also been done on the integration of data reporting crime scene detective unit equipped with internal security mechanisms. That is done in this case is the implementation of a mechanism to add security functions to the tool NuSOAP. This tool is used as authentication and confidentiality of SOAP messages that use cryptographic AES 128 [5]. Furthermore, the implementation of the user authentication for an XML document using the username token also been carried out. The trick is to do a proof of the XML document and perform validation testing of XML documents [1]. It aims to implement an XML Signature XML documents in order to obtain a secure, especially in the case of online transcript. Transcripts obtained will have a type XML digital signature contained. [6].

The next step is to implement the RSA algorithm for public key pairing and private keys for encryption and decryption process. RSA also play shows the range of data that can be processed further. Next is to implement message digest hash function SHA-1 is used for signing the XML document [7]. In other studies we can learn about the XML data that is encrypted using RSA public key algorithm with the results of its implementation in the form of two computer programs, namely findkey.exe and crypto.exe created using the C programming language [8].

3 METHODE

3.1 System Analysis

In general, the system to be built in this research is the security of data on the web service by using XML Encryption and RSA cryptography. In cryptography, RSA utilize XMLSEC library for making public key pair. Furthermore, to generate the username token also use RSA-SHA1 algorithm. This study also analyzes the system needs to be implemented, the use of functional requirements. In implementation, the web service will be divided into two parts, namely:

a. Generate web service client request, this phase deals with the processes performed by the client to make the request to the web service.

b. The server authenticates the client and returns the response. This stage describes some of the processes performed by the web service after receiving a SOAP Request from the client. Processes that occur include ensuring the integrity of the message, use the username token to authenticate users, encrypt and decrypt xml data xml data using XML encryption.

3.2 System Designing

Application system will be built have general security architecture shown in Figure 1. As every client request will be made authentication and confidentiality. Authentication is performed when the client successfully login and be granted access to resources in accordance with the right of access, confidentiality while in use in the process of encryption and decryption.

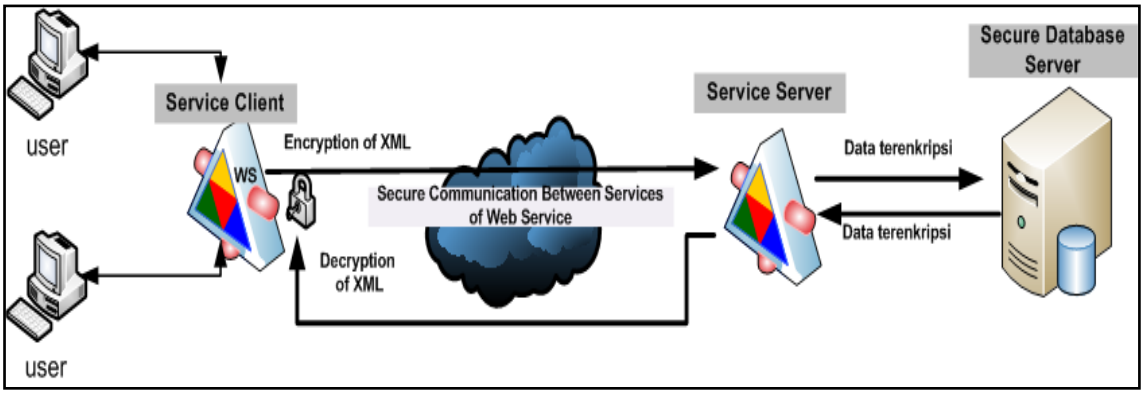


Figure 1. Model Security Service between Client and Server service from a Web Service

Figure 1 shows a model of web service security between client service and server service. Where an overview of the security system starts sending data from the user using a protocol http to client service, at this stage the data will be encrypted using the private key that belong to each user and public key, thus the xml data flowing on the communication between the client service with the web service server service from

the next in a safe (encrypted). Then the encrypted result data will be saved in a secure database with XML data formats. Decryption process itself will be performed when data is requested by another user using the user's private key and the public each key.

Designing data security mechanism is intended to provide an overview of data privacy in the process of encryption and decryption processes involving RSA public key algorithm. Encryption occurs between client service, and a server service which aims to secure the transmission line to the web service itself. This design can be shown in Figure 2.

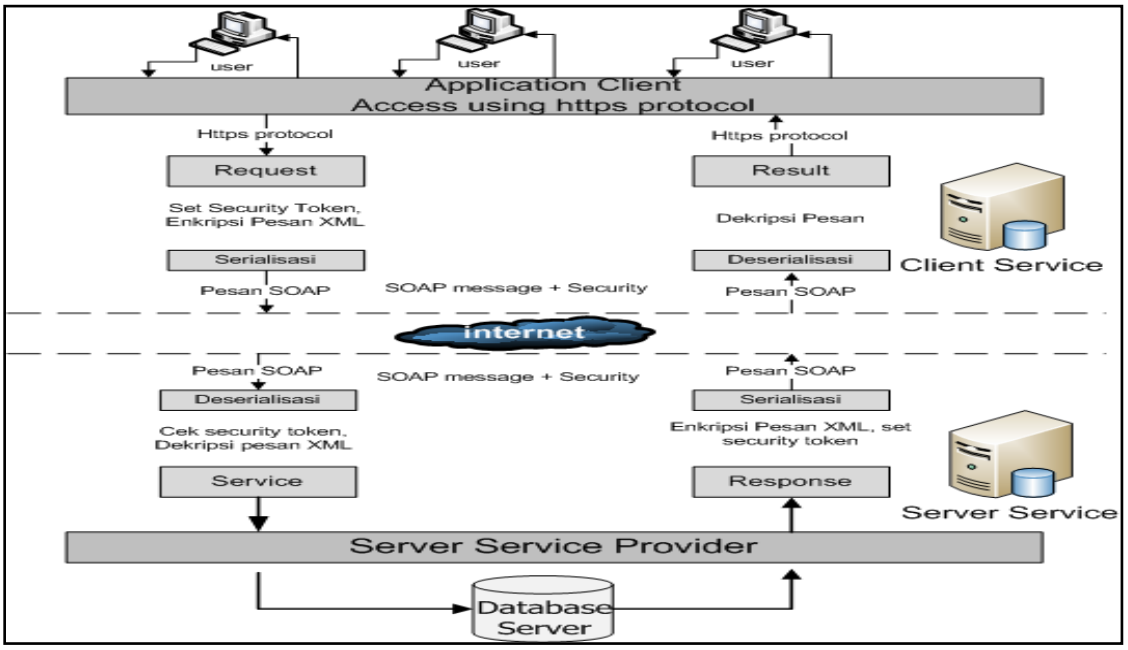


Figure 2. User Data seacret mechanism plan in web service

The implementation of the SOAP message security architecture design will be adapted to NuSOAP framework mechanism by adding a library that contains several functions that are used to support web service security in the transport path. In addition to be able to achieve the goal of security will be carried out modifications to the routine of the functions in the class library NuSOAP and regular additions of other programs for the purposes of web security service.The addition of regular programs and security functions are intended to achievement of the desired level of security messages, which in turn can do the following:

1. The ability to be able to secure the data transmission path to the web service by using a security token that is included in the SOAP Header request, the aim is to authenticate the identity of users who request service and access control to determine whether the user is served or not.
2. Ability to maintain confidentiality and authenticity of data in a SOAP request and SOAP message response. This capability is supported by the addition of a few library

of XMLSEC for encryption, decryption, and digital signature which algorithm utilize cryptography RSA 1024-bit key length.

3.3 System Implementation

Once the system design is done, the next step is to make the implementation of the security system in the Web Service. For the implementation of web service security, it designed architecture and the specific scenario in the groove as shown in Figure 3.

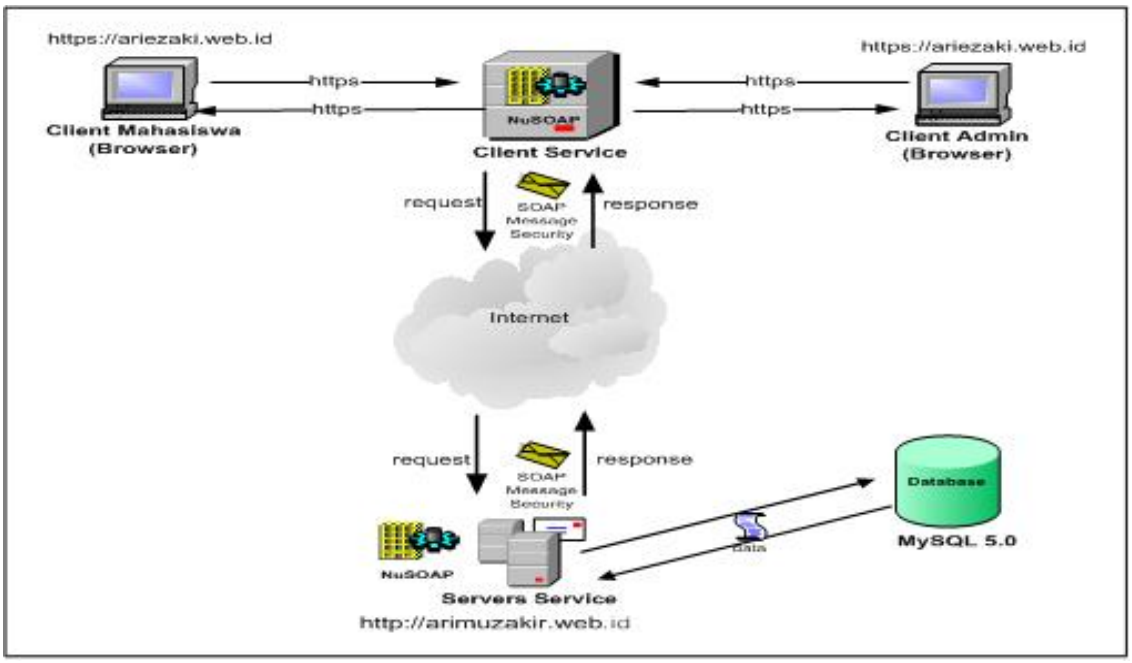
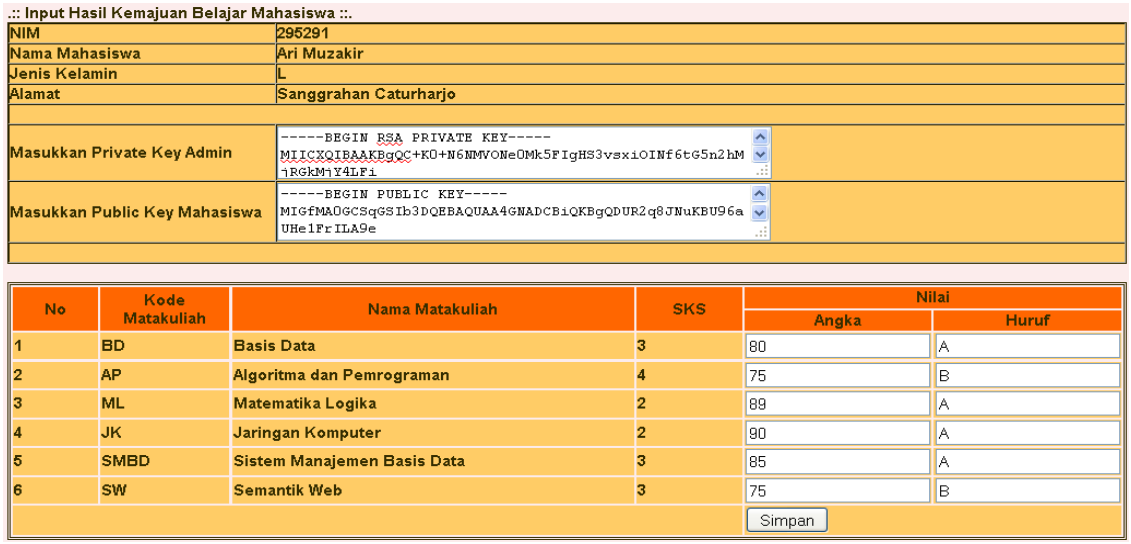


Figure 3. Implementation of web service security architecture scenario

4. RESULT AND DISCUSSION

System testing is a critical element in the development of a software tool (software) because it represents the end result of the application requirements specification, design and implementation. The main purpose of the testing system is to ensure that the relationship between the application module meets the requirements specification and according to the scenarios that have been described previously. Implementation is shown in Figure 4 in the form of application data values in data security systems XML web service, in which the figure shows that the user needs to enter his own private key and a public key to encrypt the data to be transmitted.



.:: Input Hasil Kemajuan Belajar Mahasiswa ::.

NIM	295291
Nama Mahasiswa	Ari Muzakir
Jenis Kelamin	L
Alamat	Sanggrahan Caturharjo
Masukkan Private Key Admin	-----BEGIN RSA PRIVATE KEY----- MIICXQIBAAKBgQC+KO+N6NMVONeOMk5FIgHS3vsxiOINf6tG5n2hM jRGkMjY4LFi
Masukkan Public Key Mahasiswa	-----BEGIN PUBLIC KEY----- MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDUR2q8JNuKBU96a UHe1FrILA9e

No	Kode Matakuliah	Nama Matakuliah	SKS	Nilai	
				Angka	Huruf
1	BD	Basis Data	3	80	A
2	AP	Algoritma dan Pemrograman	4	75	B
3	ML	Matematika Logika	2	89	A
4	JK	Jaringan Komputer	2	90	A
5	SMBD	Sistem Manajemen Basis Data	3	85	A
6	SW	Semantik Web	3	75	B
				Simpan	

Figure 4. Trial Web Security service in the data value

The results obtained in Figure 4 is the xml data security in web services are tested on student data values. The results of the testing focused on confidentiality and data integrity. In the testing phase of this confidentiality, client service will encrypt the SOAP message to be sent is the data to be sent by calling the encryption on the server and use the public key of the client, the process of encryption using the RSA algorithm with a key length of 1024 bits. While the decryption process is done on the server service by using the private key. Furthermore, to see the results of this request SOAP message that contains encrypted data using XML Encryption method shown in Figure 5 below.

```
<SOAP-ENV:Body>
<EncryptedData xmlns="http://www.w3.org/2001/04/xmlenc#"
Type="http://www.w3.org/2001/04/xmlenc#Element">
            <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-
cbc"/>
            <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
            <EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#">
                        <EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>          <KeyInfo
xmlns="http://www.w3.org/2000/09/xmldsig#">
                        <KeyName/>                  </KeyInfo>
                        <CipherData>
            <CipherValue>ill9Dz2IXkJuQ9Nrkdqup/4I/npZeywQIfivHO4MTEmXRYIBOVi
SpNROeKKcBNRLthH8ROQsdpTiN/7kO+ppfCBqjX+j9mGEHJOS+U0Tp9KqxFeN4YR3bJ
W4Lt/VOpxvVy+3TnGTv4cZxB0emNcR3H2BUYtjMen65aIflP5wa8=</CipherValue>
                        </CipherData>
                        </EncryptedKey>
            </KeyInfo>          <CipherData>
            <CipherValue>5BzJItoZ9gMD8pmjNbGg2ynQZR9jYVtmz3YQVHaE6jyMECV1
MXlFNKya13EoO7nCojzq3z03mSXXHC2CFrQkBW3R6pDFHTJqzc8i6he1VLOpcfz+J29A
HlswhdVR50RGW2emplnvGawsAD4zlVO15Uy9n010ZLDYL9sOB/MHe+Pk/hwTn0bu1Cel
7tk5kiBqH1865H3868mmVenKJaISjgHulhqZtX</CipherValue>
            </CipherData>
</EncryptedData>
</SOAP-ENV:Body>
```

Figure 5. The soap request Results Message Using XML Encryption Security Model

The result of Figure 5 above is: all data is encrypted by the client service to ensure the confidentiality of data on transmission lines to the web server service. Then when the data is sent, the client will call the security functions in the client service named library class_wss.php, then when the data is sent from a client service, then the data will be encrypted SOAP.

While the client to the server authentication using security tokens expressed in a SOAP message request. If the username token in client service with username token in the server service, the client service can be allowed to access the service in accordance with the value of the parameter that has been inserted in the header. Username token itself is encrypted using the SHA1 algorithm; the results are as shown in Figure 6.

```
<SOAP- ENV:Header>
<wsse:Security xmlns:wsse="http://schemas.xmlsoap.org/ws/2003/06/secext">
            <wsse:UsernameToken">
              <wsse:Username>8a9a3d2ab453f7a407d97db5e16d6c0274e92f</wsse:Username>
              <wsse:Password
Type="wsse:PasswordDigest">05f19383099ed3304153baeb08a8bd9ffd8a0</wsse:Password>
              </wsse:UsernameToken>
</wsse:Security>
</SOAP-ENV:Header>
```

Figure 6. Soap request result with Token username

Besides authentication can also be done by checking the authenticity of a SOAP message (verification) that is sent in the form of digital signatures, the results obtained are valid and invalid. Figure 7 shows the appearance of the authentication process by checking the username token and verify the authenticity of the received data on the web server service. The results of the authentication and verification of this will be written to a file called "logverifikasi.txt".

```
14-01-2012 12:20:46
otentikasi sukses
verifikasi sukses
14-01-2012 12:27:51
otentikasi sukses
verifikasi sukses
14-01-2012 13:41:07
otentikasi sukses
verifikasi sukses
```

Figure 7. Log Results Authentication Security Token Checking

5 CONCLUSION AND RECOMMENDATION

5.1 CONCLUSION

1. The design and implementation of modules that have been done using the security and support of the library as a library supporter XMLSEC library and library built class_wss able to address the security issues in the delivery of a security authentication, authorization, and confidentiality of SOAP request message generated.
2. Results of the implementation indicate that confidentiality can be solved by applying the concept of security based on the security of XML Encryption library. The results of the SOAP message request in the delivery process can

meet the standards of web security service, where the data as it is transmitted in an encrypted using class_wss library has been built.

3. Tests were done on web service by applying a model library as a library security class_wss web service that is built gives good results, ie SOAP request messages when sent in an encrypted form and be able to be decrypted..

5.2 RECOMMENDATIONS

Key exchange in this study was limited prototype so for the future need a more secure key exchange, such as the server key is stored in a separate repository database server in order to more gate.

REFERENCES

[1] Rakhim, R, T, 2010, Keamanan *Web Service* Menggunakan Token, Tesis S2 Magister Ilmu Komputer, Universitas Gadjah Mada, Yogyakarta.

[2] Zhang, W., 2009, Integrated *Security* Framework for Secure *Web Service*s, Research Institute of Applied Computer Technology, China Women's University.

[3] Adriansyah, A, Arifandi,W, dan, Wicaksono, N , 2005 ,*Keamanan Web Service*, Teknik Informatika, Institut Teknologi Bandung, Bandung.

[4] Fareghzadeh, N,(2009), *Web Service Security Method To SOA Development*, World Academy of Science, Engineering and Technology, No.49, 10 hal.

[5] Kenali, E., W., ,2010, Implementasi *Web Service* untuk Integrasi Data Satuan Reserse Kriminal (Studi Kasus Polda Lampung), Tesis S2 Magister Ilmu Komputer, Universitas Gadjah Mada, Yogyakarta.

[6] [6] Suteja, B ,2004, Implementasi XML Signature untuk Secure XML Pada Kasus Integritas Transkrip Online, Tesis S2 Magister Ilmu Komputer, Universitas Gadjah Mada, Yogyakarta.

[7] Supriyanto,A., 2007, Otentikasi Dokumen XML menggunakan Algoritma RSA dan Hash SHA-1, Tesis S2 Magister Ilmu Komputer, Universitas Gadjah Mada, Yogyakarta

[8] Hartono, B., 2003, Pemakaian kriptografi kunci publik dengan algoritma RSA untuk keamanan data XML, S2 Ilmu Komputer, Universitas Gadjah Mada, Yogyakarta.