Digital Certificate Exchange of Agricultural Products using SOAP Web Services

Miyanda Chilikwela[1]
Department of Electrical and Electronics Engineering
University of Zambia, Lusaka, Zambia

Jackson Phiri[2]
Department of Computer Science
University of Zambia, Lusaka, Zambia

***Abstract*—Developing countries have continued to experience a number of challenges in managing import and export certificate for various goods. In this paper, we are proposing a model for digital certificate exchange in an effort to improve the security levels of data exchange among the government organizations and the business community. With the increase of various information systems being used in many organizations, data exchange between systems has become critical. The model developed uses SOAP web services for data exchange and RSA encryption for secure data exchange. Ministry of Agriculture is responsible for the issuance of import and export certificates in Zambia while Zambia Revenue Authority is responsible for ensuring that goods imported or exported out of the country have a valid certificate that is authentic. The results show that the model provides a secure and timely exchange of information between the ministries and the government agencies.**

***Keywords*—Digital; certificate; Rivest, Shamir and Adleman (RSA); Simple Object Access Protocol (SOAP); web service; model**

I. Introduction

The government of the republic of Zambia has appointed the Ministry of Agriculture (MOA) and other related ministries to oversee the import and export of certain controlled products such as food through the issuance of import and export certificates prior to the importation or exportation of goods [1]. The ministries are responsible for ensuring that the products imported or exported have a valid certificate prior to importation or exportation [2]. There are various agencies that are tasked to ensure that the certificates issued are valid at the time of import or export. Such agencies include Zambia Revenue Authority (ZRA) which is mandated to collect taxes on behalf of the government [3]. The authority depends on the certificates presented to them by would be exporters or importers during the importation or exportation of goods.

The certificates presented are sometimes forged or expired certificates. This results in the importation or exportation of food stuff that don't meet health requirements. This consequently has adverse effects on health. The lack of secure data exchange results in forged certificates being presented to the authority at the boarder points and loss of government revenue [4]. Therefore a proposed model which uses SOAP web services in the exchange of information between government agencies and ministries will be used as a means of data exchange. The model is based on ISO 27001 standard to ensure that data being exchanged is secure. This paper is structured as follows: Section II looks at the literature review, followed by Section III which shows related works. Section IV focuses on the methodology, Section V looks at the security mechanism. And finally in Section VI, the findings are presented and conclude the paper in Section VII.

II. Literature Review

A. Ministry of Agriculture

The ministry is mandated to design, implement and manage the Governments activities in the agricultural sector. The purpose of the ministry is to facilitate and support the development of a sustainable, diversified and competitive agricultural sector that assures food and nutrition security, contributes to job creation and maximizes the sector's contribution to Gross Domestic Product. The ministry is mandated under the Control of Goods Act to ensure that controlled goods being imported or exported into the country meet the stated requirements as per the law [1].

B. The Control of Goods Act

The control of goods act is an act that provides regulation of the sale, distribution, purchase and disposal of unmanufactured or manufactured products or poultry and animal. The act controls the import and export of controlled products such as poultry or animal and other products [2].

C. Web Services

A web service is any service that is available over the Internet, uses a standardized (Extensible Markup Language) XML messaging system, and is not tied to any one operating system or programming language specification. Web services use Hyper Text Transfer Protocol (HTTP) for data exchange. Web services employ a variety of technical standards such as XML, Simple Object Access Protocol (SOAP), Web service Description Language (WSDL), Representational State Transfer (REST) and Universal Description, Discovery and Integration (UDDI) [5] [6]. Fig. 1 shows data exchange between different systems.

D. SOAP Web Services

SOAP is a protocol based on XML for exchanging information between computers. Because SOAP is platform-independent it enables applications or systems written in different programming languages to be able to communicate. The WSDL is an XML vocabulary used to describe SOAP-based web services. XML is a language that uses XML tags to describe the data being exchanged [5].

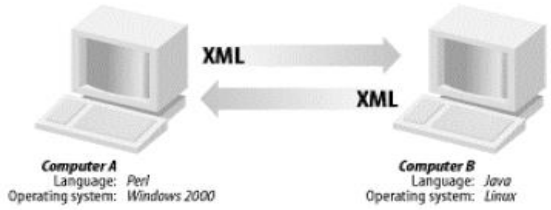

Fig. 1. Web Service [5].

E. ISO 27001 Standard

ISO stands for International Standard Organization; it was formulated to provide a model for establishing, implementing, operating, monitoring, reviewing and maintaining an Information Security Management System (ISMS). The standard emphasizes implementation of operating controls that manage an organization's information security risks in the context of the organization's overall business risks among others. This includes measures or controls put in place by an organization to safeguard itself from different types of threats. The control objective: "*to maintain the security of information and software exchanged within an organization and with any external entity*" seeks to ensure that information being exchanged is secure during transmission. This includes all forms of controls put in place to safeguard data in transit against cyber-attacks [6] [7].

F. Encryption

Encryption refers to the art of protecting information by converting the information into an unreadable format. The encrypted text is called cipher text [8]. Encryption algorithms can be categorized into two types, namely Symmetric and Asymmetric keys encryption. Encryption where one key is used to encrypt and decrypt data is known as Symmetric keys encryption. In Asymmetric keys, two keys are used; private and public keys [8] [9]. There are many cryptography algorithms used to secure information such as RSA, 3DES, Blowfish, AES, DES, Paillier and ElGamal. The user who wishes to implement encryption needs to find the best security algorithm which consumes less computational power and provides high security [10] [11].

G. RSA Encryption

Rivest, Shamir and Adleman (RSA) introduced RSA algorithm in 1977. RSA is an asymmetric algorithm that uses the public key for encryption and the private key for decryption as shown in Fig. 2 [12]. RSA key generation is generated as follows.

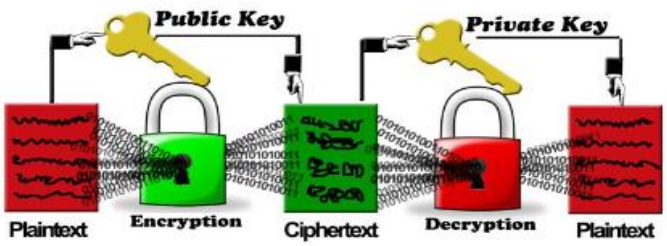

Fig. 2. RSA Encryption and Decryption [14].

Taking two large prime numbers (P and Q), Computing N by using the given formula (N=P* Q), Choose the public key exponent E such that 1 < E < (N) and, E and (N) are co-prime. Finally determine the private key exponent D through the given formula. D *E= 1*mod ((N)). The public key consists of (N, E) and the private key consists of (N, D) [13].

Current usage of RSA: Pretty Good Privacy (PGP) is a freeware that provides encryption and authentication for email and file storage applications across multiple platforms and uses RSA algorithm for transporting the key. Googles G Suite, is a brand of cloud based services that provides collaboration tools, products such as Gmail, Hangouts, Calendar [13].

Strengths of RSA: The strengths of RSA lies in the use of large random prime numbers to calculate the modulus. It is difficult to computationally factor large integers into primes. Keys of size 2048 bits provide best security. It is widely used for secure communication channel and for authentication to identity service provider [13] [14].

Husam Ahmed Al Hamad alludes to the use of XML for exchange and integration of data between heterogeneous applications and systems. XML represents data using tags called elements. Each data component to be exchanged is represented by a tag. The author suggests that XML has become a standard data format that is widely used by many organizations and a common language for data transmission over the Internet [15].

Marcelo arenas pontificia and Leonid Libkin discuss the use of XML to exchange data due to the increased need for exchange of data in various formats. The advantages of XML that makes it suitable for data exchange include the format of XML document is not rigid, can easily add additional information using the elements [16].

Cui-xiao Zhang, Ying-xin hu, Guo-bing Zhang and Jin Sha define web services as a technique to achieve data exchange. The authors further state that web services not only provide the possibility of data exchange, but also provide the technique supporting data integration, data collection and data sharing between different systems. Web services provide a valid technique support for system integration [17].

P. Dinesh, P. J. Charles and S. BrittoRamesh narrate that web services is a self-contained, self-describing and modular applications that can be described, published, located and invoked over a network . Web services provide means for data exchange that can be written in a different programming language from that of the exchanging parties [18].

Douglas Harris, Latifur Khan, Raymond Paul and Bhavani Thuraisingham discuss that data integration has been at the core of research until recently where brute force integration techniques that consisted of techniques such as gateways and translators were used between multiple data management. Standards such as Remote Database Access (RDA) were developed initially for client- server interoperability. Later object-based wrappers were used to encapsulate the multiple systems including the legacy systems. The authors allude that common representation of the data remained a challenge [19].

Rajdeep Bhanot and Rahul Hans carried out an analysis on various encryption algorithms based on different parameters. The authors proceeded to compare the algorithms to choose the best algorithm. They defined RSA as the most important public-key cryptosystem. The RSA algorithm can be used for digital signatures and public key encryption. The security is based on the difficulty of factoring large integers [8].

III. Related Works

Rajan Datt, N.N. Jani, Rasendu Mishra, Ajay Patel designed a model using web services to exchange data between the heterogeneous databases. The findings of this study are that web services are being employed as a means of exchanging data between heterogeneous databases. The model developed does not secure data being transmitted over the web. It is on this basis of limitation that this research is being conducted [20].

Aftab Ahmed Chandio, Dingju Zhu, Ali Hassan Sodhro and Muhammad Umer Syed proposed a system for the University of Sindh based on the Service Oriented Architecture (SOA) with web services. The system solves the problem that frequently occurs in the process of no-dues verification of a student from different departments. No security mechanisms were implemented to safeguard the data whilst in transmit over the web despite the websites being used within the organization. This limitation provides the basis for this research [21].

P. Dinesh, P. J. Charles and S. BrittoRamesh reviewed related works based on the studies of ten different authors. Their works review different security mechanisms that can be employed in web services. They further outlined that public key infrastructure security mechanism provides device and service authentication [18]. This research seeks to implement asymmetric type of encryption.

Vu Van Tan, Dae-Seung Yoo, and Myeong-Jae Yi designed and implemented a web application-based OPC (Openness, Productivity, and Connectivity) technique to exchange data between the measurement and control systems on the plant floor with XML for slow process monitoring and control systems. The solution fully applies technologies such as OPC, XML, and links to the Internet [22].

Memorie Mwanza and Jackson Phiri conducted a research study on fraud detection on bulk tax data using Business Intelligence (BI) data mining tool. The authors outlined that ZRA like many other revenue authorities in Africa, has been affected by fraud mechanisms employed by tax payers. They identified BI as a technique that can be used to detect tax frauds, non- fillers and non- compliant tax payers. They further alluded that data mining is a significant technique that can be used to overcome the challenges of fraud detection and anomalies that arise in tax administration [23].

Jackson Phiri and Tiejun Zhao study was on identity attributes using quantitative analysis and developed an identity attribute metric model. The study focused on various sources of information such as first name, last name, email address and date of birth that can be obtained from various forms i.e public services, health care systems. The model seeks to improve the robustness of most identity systems [24].

IV. Methodology

Qualitative research was primarily used to gather information on the import and export of agricultural products. Techniques such as observations and record sampling were employed. Activities involved mapping of the current business process that highlights the process flow from import application to actual importation of products in part (a). The proposed business process is then highlighted in part (b) below. The model is developed in java based on the proposed business process as shown in part (d). To evaluate data exchange, an application for a certificate is approved and data is electronically submitted on the customs processing system for import approval at the border office.

The following activities were carried out in the methodology:

A. Mapping of Current Business Process Flow

The interaction of the importer/exporter in the importation and exportation of goods includes various business processes from MOA and ZRA. Fig. 3 below shows the use case diagram and interaction of the actors in the current business process.

- Current business Process

The current business process flow for the importation and exportation of goods is described below as shown in Fig. 4.

An importer or exporter obtains an application form from MOA. He/she fills in the form and submits it to the Senior Agribusiness Officer at MOA. The officer verifies the quantity applied for importation or exportation. The quantity applied for depends on the product being imported or exported. If the verification results are successful, the importer or exporter is advised to make a bank deposit for the certificates applied for. The importer or exporter makes a bank deposit and presents the bank deposit slip to the Officer at MOA. The officer proceeds to approve and issue the certificates based on the quantity applied for. The certificate issued is only valid for 30 days from the time of issuance there after it is deemed as invalid.

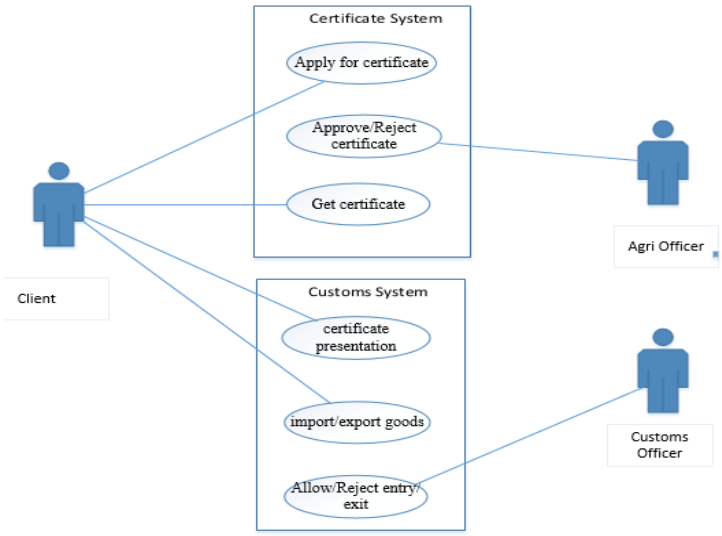

Fig. 3. Use Case Diagram of Current Business Process.

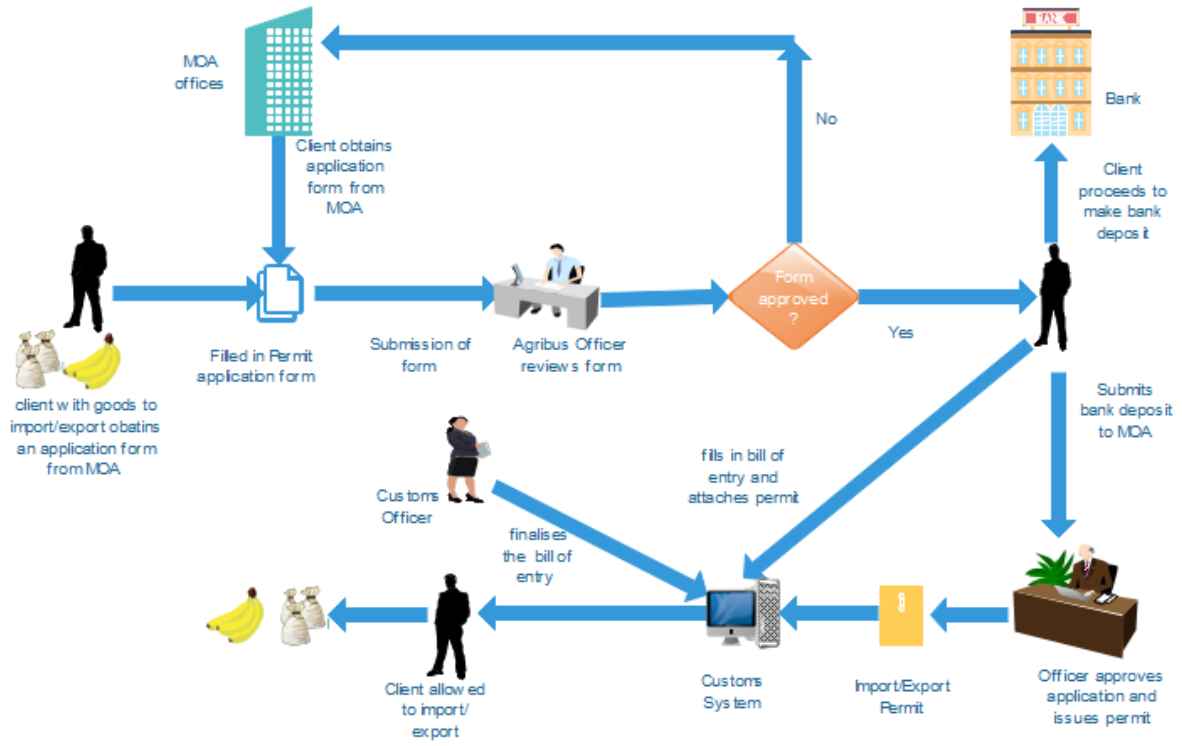

Fig. 4. Current Business Process.

The importer or exporter proceeds with the clearing process on the customs system. He/she scans the certificate(s) and attaches the certificates to the bill of entry on the customs system. Then he/she finally registers the bill of entry as a submission to import or export goods. The customs officer scrutinizes the bill of entry on the customs systems. If the attached certificates are not valid the importer/exporter is asked to obtain valid certificates from MOA.

The certificate presentation by the importer/exporter and the validation process by the customs officers is manually done.

According to the Control of Goods Act [2], a potential importer/exporter who wishes to import or export goods needs to obtain a valid import or export certificate prior to the importation or exportation. The steps followed are:

1) The applicant applies for a certificate to import or export

2) If the applicant meets the requirements, the applicant pays the required amount.

3) Client is issued with import or export certificate.

4) Client presents the certificate at any of the customs boarder offices in the country.

5) ZRA customs officer checks if the certificate is valid

If it's valid, client is given the opportunity to export or import their goods.

- Challenges of the Current Business Process

The paper based system that is used for the exchange of certificate data between the government agencies has the following challenges:

1) Certificates presented at the boarder offices may not be genuine (counterfeit certificates).

2) Loss of government revenue because some clients use old certificates during importation or exportation.

3) Lack of physical presence of trained man power from Ministry of Agriculture at all boarder offices in the country.

4) Customs officers are not trained to validate the authenticity of the certificate thus they are unable to identify potential culprits.

5) Importation or exportation of banned goods that may pose health challenges.

B. Proposed Business Process

An importer or exporter applies for a certificate on the certificate processing system website. The officer then verifies the quantity applied to be imported/exported. The importer or exporter is advised to make a bank deposit for the certificates applied for. The importer or exporter makes a bank deposit and presents the bank deposit slip to the cashier at MOA. The cashier inputs the bank deposit slip details and submits the application. The Agribusiness Officer proceeds to approve the certificate, clicking the approval button invokes the web service as shown in Fig. 5. The SOAP request message with the certificate details is created as shown in Fig. 6. Once the SOAP request message is created, it is encrypted and sent to the Customs System. The SOAP request message is received on the customs system where the message is decrypted and a SOAP response message is sent to the certificate system. The client uses the digital certificate received on the Customs system to frame the bill of entry.

- How it works

The development and implementation of the soap web service included the following activities:

1) Creation of a user requirements document that defined data to be exchanged between parties.

To develop, implement and use soap web services, a contract (WSDL) needs to exist between the two parties that need to exchange data. The contract defines the data elements to be exchanged, the purpose and function of its operations, messages that need to be exchanged in order to engage the operations, a set of conditions under which the operations are provided and information about how and where the service can be accessed. The user requirements document is signed by both parties.

2) Development of a SOAP web service by both parties based on WSDL.

The web server and web client was developed in java programming language. The system that provides a resource becomes a client and the system that utilizes the resources sent is the server. The Certificate Processing System is the client while the Customs System is the server. The Customs System has a web service that defines the data it is expecting to receive. The Certificate Processing system has a web client that sends certificate data to the Customs Processing System.

```
public static void main(String args[]) {

    SwInfoDetails sw = new SwInfoDetails();
    sw.SendPermitDetails(15);
}
```

Fig. 5. Java Code.

The sw object shown in the fig above contains data that is sent from the Certificate Processing System. The object contains data such as the goods code, description, permit number and importer/exporter code as shown in Fig. 6. Once the object is compiled it creates a SOAP request message as shown in Fig. 6. The message contains the data elements generated from the client.

1) The SOAP request is successfully sent to Customs System where it is saved on the database and a SOAP response is sent back to the client as shown in Fig. 7.

2) SOAP response message sent back to Certificate Processing System.

Fig. 8 shows the SOAP response message that is generated on the server side once the SOAP request message is received from the client. The certificate number is used on the customs processing system when importing or exporting goods.

C. Security Mechanism

The SOAP request message is encrypted using RSA encryption. To encrypt the data, there is need to have a public/private key pair. The key pair consists of the public key and the private key. To generate the key pair, a keystore is created using the keytool JDK utility as shown in Fig. 9 below. This file has both per-store and per-key passwords which provides additional security to the key pair.

```
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/">
<S:Body><ns2:swSubmit
xmlns:ns2="http://www.asycuda.org"><ns2:swInfo>
<ExpCode/><ExpNam/>
<ImpCode>1000001420</ImpCode>
<ImpNam>JONES MWANGALA</ImpNam>
<CuoCod>VFL</CuoCod>
<RefNbr>I201803VFL0003</RefNbr>
<GoodsItems>
<GoodsCode>10051000000</GoodsCode>
<GoodsDescription>Maize seed</GoodsDescription>
<Quantity>458</Quantity>
<Weight>458</Weight>
<Value>4544 ZMK</Value>
<Unit> </Unit>
<QuotaUsed>0.0</QuotaUsed>
<QuotaBalance>458.0</QuotaBalance>
<PerNbr>I201803VFL000310051000</PerNbr>
<PerValidFrom>14-Mar-18</PerValidFrom>
<PerValidTo>13-Apr-18</PerValidTo>
<Origin>AE</Origin>
</GoodsItems>
<Agencies>
<AgencyName>Ministry of Agriculture</AgencyName>
<AgencyDetails>Ministry of Agriculture</AgencyDetails>
<Status>Processed</Status>
<Comment>ok</Comment>
</Agencies>
<Agencies>
<AgencyName>Ministry of Agriculture</AgencyName>
<AgencyDetails>Ministry of Agriculture</AgencyDetails>
<Status>Processed</Status>
<Comment>okay</Comment>
</Agencies>
</ns2:swInfo>
</ns2:swSubmit>
</S:Body>
</S:Envelope>
```

Fig. 6. SOAP Request Message.

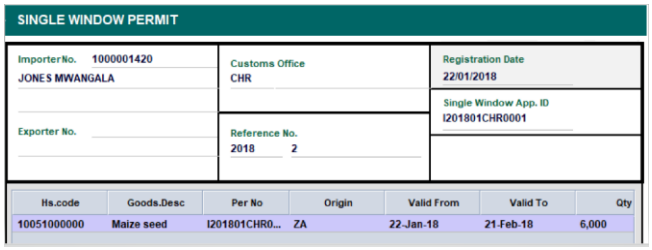

Fig. 7. Digital Certificate Data on Customs System.

```
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/">
<S:Header/>
<S:Body><ns2:swSubmitResponse
xmlns:ns2="http://www.asycuda.org">
<ns2:swSubmitResult>
<result>E</result>
<errorCode>0</errorCode>
<ErrorDescription>Permit Sent Successfully</errorDescription>
</ns2:swSubmitResult>
</ns2:swSubmitResponse>
</S:Body>
</S:Envelope>
```

Fig. 8. SOAP Response Message.

```
C:\keystore>keytool -genkeypair -alias mykey -storepass s3cr3t -keyalg
RSA -keystore keystore.jks
```

Fig. 9. Keystore Generation.

```
C:\keystore>keytool -export -file miyanda.cer -alias mykey -storepass s3cr3t -
keystore keystore.jks
Certificate stored in file <miyanda.cer>
```

Fig. 10. Key Pair.

The key pair is generated as shown in Fig. 10. The key store directory contains the miyanda.cer file which contains both the public and private key as shown in Fig. 11.

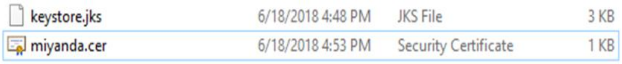

Fig. 11. Keystore Directory.

The miyanda.cer file below in Fig. 12 shows the encryption algorithm, and the signature hash algorithm.

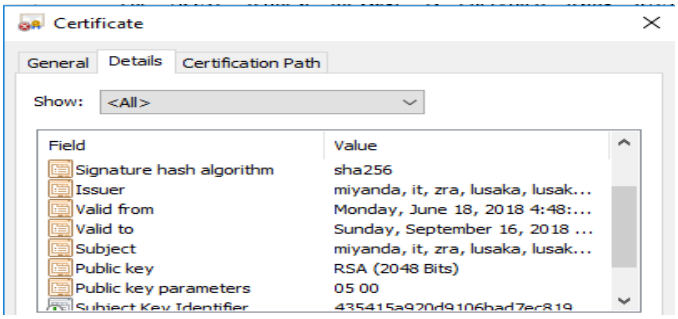

Fig. 12. Certificate Contents.

Fig. 13(a) below shows the flowchart for the generation of the keystore using keytool JDK utility.

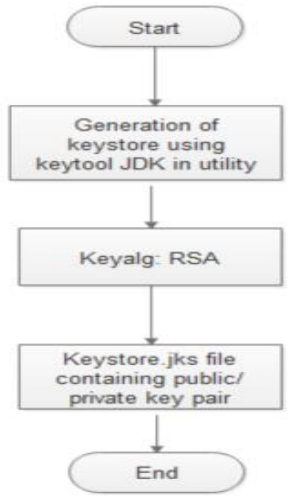

Fig. 13 (a). Flowchart for Keystore Generation.

Algorithm for the generation of encrypted SOAP request using the public key is as follows:

Algorithm 1: At Client Side

Input: SOAP request message

Processing: encryption of SOAP request message using public key

Output: encrypted SOAP request message

Fig. 13(b) shows the flowchart for the generation of encrypted SOAP request message.

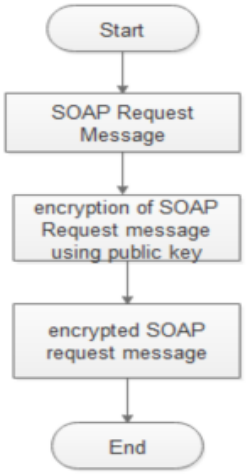

Fig. 13 (b). Flowchart for Encryption of SOAP Request.

Algorithm 2: At Server Side

Input: encrypted SOAP request message

Processing: decryption of SOAP request message using private key

Output: decrypted SOAP request message in customs processing system

Fig. 13(c) below shows the flowchart for the decryption of the encrypted SOAP request message.

Fig. 14 shows the proposed business process.

Fig. 13. (c) Flowchart for Decryption of SOAP Request.

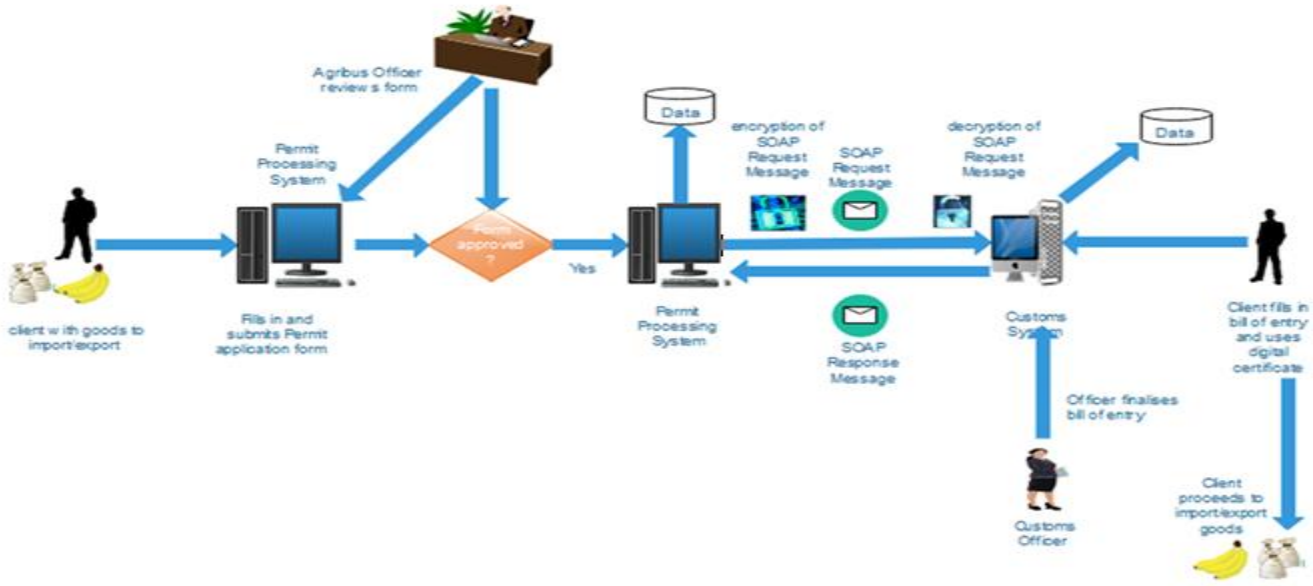

Fig. 14. Proposed Business Process.

D. Proposed SOAP Web Service Model

To achieve secure data exchange between MOA and ZRA the following model is proposed.

1) The client applies for a certificate through the electronic Certificate Processing System.

2) MOA approves the clients certificate.

3) Upon approval of the certificate, the data about the certificate is encrypted and sent to ZRA's system via SOAP web services.

4) The cleint then finds the approved certificate on the Customs Processing system and uses the certificate to declare the goods to be imported or exported.

Components of the SOAP web service model

1) Certificate processing system: The application system used for processing of certificates is developed in Java programming language. The MOA has a web service client written in java programming language that will invoke the web service at ZRA. The web service will only be invoked once the certificate has been approved. Once the certificate is approved a SOAP request message will be sent to the Customs Processing System.

2) Customs processing system: The system used for declaring goods to be imported or exported is developed in java programming language. The authority has a web service server written in java programming language. The server will be receiving certificate data sent in XML format from MOA certificate processing system. The system will respond with an appropriate SOAP response.

3) The SOAP web service: The web service model is written in java programming language and consists of XML tags that define the data being exchanged. The SOAP web service has a WSDL that defines the standard data that is being sent from one system to the other. The web service model defines the expected request and response. Fig. 15 shows the WSDL of the SOAP web service. The WSDL is the contract that shows the data to be exchanged between the two systems. It shows the individual fields to be exchanged.

4) Database systems: The database management system being used by both parties is Oracle 11g. The certificate processing system will store certificate data in the database. Once the SOAP request is sent to the Customs Processing System. The certificate data is stored in the oracle database for the customs processing system.

5) Web: The web is an interconnection of specially designed web pages. These web pages are specially formatted using HTTP. The SOAP request is moved via the web from one system to the other.

V. System Architecture

The architecture has five main components these are (Fig. 16):

1) The Certificate Processing System
2) The SOAP web server and the database storage
3) The web
4) The Customs System
5) The SOAP web client and the database storage

The SOAP request is sent via the web to the Customs System where it is saved to the database and a SOAP response is sent back to the Certificate Processing System.

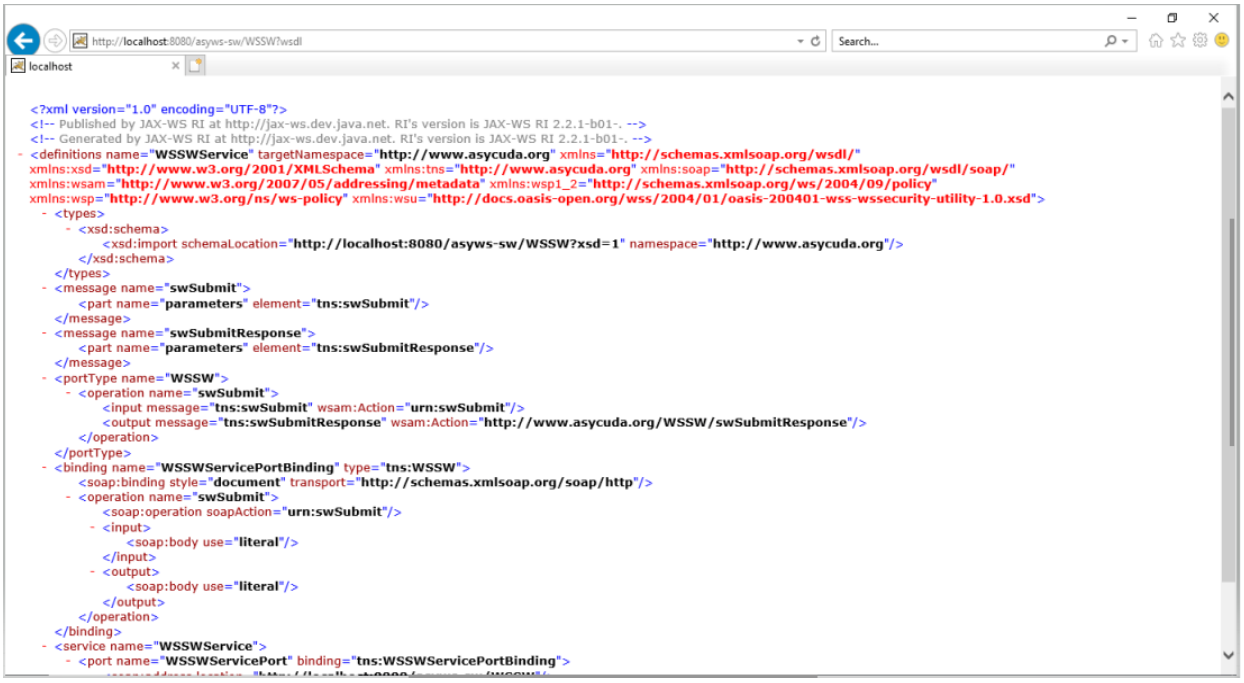

Fig. 15. SOAP Web Service (WSDL).

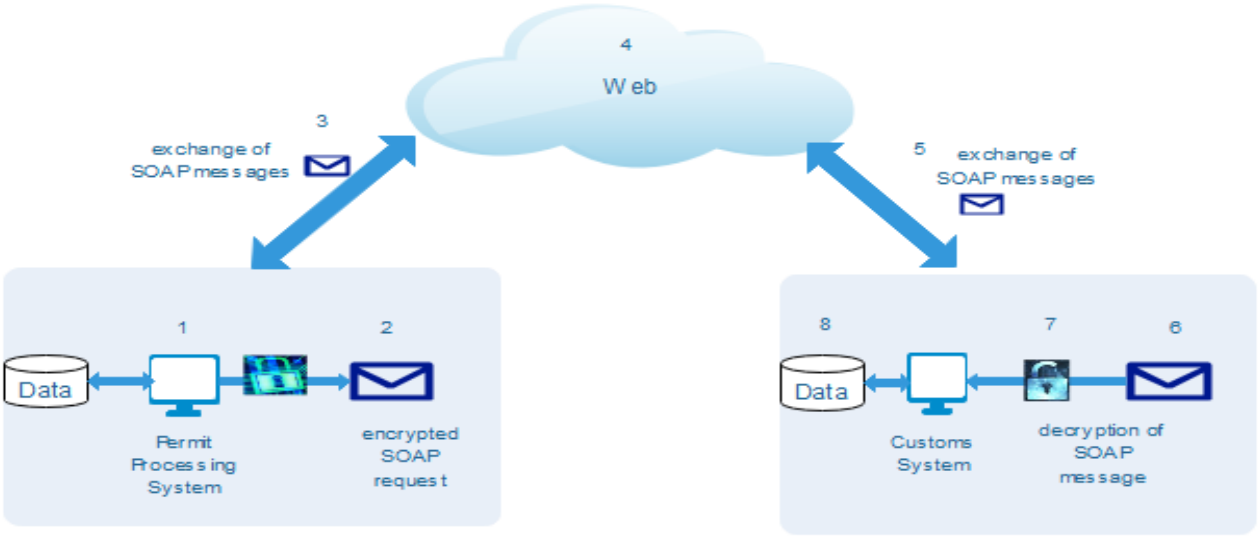

Fig. 16. System Architecture.

VI. Results and Discussion

In the prototype developed, an application for a permit was submitted on the Certificate Processing System which was approved. Once the officer clicked the approval button the web service is invoked and a SOAP request message is generated as shown in Fig. 17. The SOAP request is encrypted and converted to an object as shown in Fig. 18.

The encrypted SOAP request is transmitted via the web and reduces the chances of data alteration, data theft because the data is encrypted using a public key. The recipient of the data uses the private key to decrypt the data. The importer/ exporter uses the received digital certificate to frame an entry on the customs processing system as shown in Fig. 19.

```
public static byte[] encrypt(String soapRequest, PublicKey publicKey) throws Exception {
    Cipher encryptCipher = Cipher.getInstance("RSA");
    encryptCipher.init(Cipher.ENCRYPT_MODE, publicKey);

    //byte[] cipherText = encryptCipher.doFinal(soapRequest.getBytes());

    return encryptCipher.doFinal(soapRequest.getBytes());
}
```

Fig. 17. Java Code with Encryption of SOAP Request

-c‰‘’
ŽµÒ½_nÌK?>3ð,,_
‘ÍA²†¼µŸ_t7_©?)}-[xÞiy_ïöTê4GÉYþ_ñÚ_Eü_?Zôª0ðñ0¸×−2ž_H_æ_>”ëD
à5›-õë,È"_ÆâUEÏV¸Ö_Î’”¦/ÉŠÛÜÊÍPe)_éãÛr›ü_£a`Ïú×Áú£ô!‰õ_r_PP}hF_
yæzSÊ}uyâ˜_õi)ª5…»Ëpƒ5s8___ö(íí¦_býh;SF_Øƒ,ó]_¢p®••dlŸOÚ4ì
_Z__F%Å¹vQì_gßç_1î?

Fig. 18. Encrypted SOAP Object.

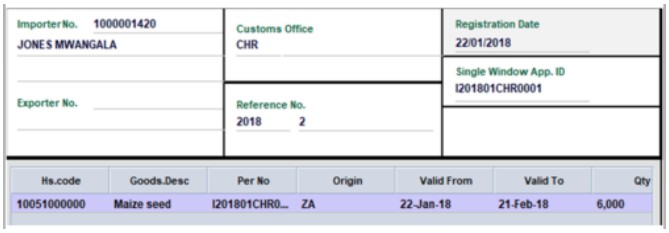

Fig. 19. Received digital certificate

This ensures that only approved certificates from the Certificate Processing System are used during importation and exportation. Clients will no longer present physical documents at the customs boarder offices. This solves the challenges of invalid certificates, forged certificates and prevents unauthorized entry of banned goods. It's important to note that a weak key generation makes RSA very vulnerable to attacks therefore care must be taken to ensure that two large random prime numbers are used to calculate the modulus.

The model can be used as a baseline model for the exchange of data/information between government agencies that wish to share information between different information systems. This model can be used as an aid to e-government. The RSA security algorithm implemented helps to achieve data confidentiality, integrity and availability of data.

VII. Conclusion

In this paper, a secure SOAP web service model has been developed. The model is used for certificate data exchange between heterogeneous systems. The model helps to solve the data security challenges being faced by many governments and organizations. The model can be used as a framework for implementation of e-government especially that the model provides a cheaper platform for data exchange.

Future work includes the exploration of penetration tests to ensure data being exchanged over the web is secure from cyber -attacks. The research can be carried out to ascertain the extent of accessing the SOAP data request being exchanged while it's in transit over the web using various packet sniffer tools.

Acknowledgment

The authors would like to thank the Zambia Revenue Authority (ZRA) and Ministry of Agriculture (MOA) for the support given during this research. Appreciation also goes to staff at the University of Zambia for the support rendered during the research.

References

[1] "http://www.agriculture.gov.zm/," [Online]. [Accessed 18 July 2018].

[2] G. o. t. R. o. Zambia, "http://www.parliament.gov.zm/sites/default/files/documents/acts/Control%20of%20Goods%20Act.pdf," Government of the Republic of Zambia. [Online].

[3] Z. R. Authority, "https://www.zra.org.zm/main.htm?actionCode= show HomePageLnclick," [Online].

[4] "http://www.times.co.zm/?p=95579," [Online].

[5] M. Z. Gashti, "Investigating Soap and Xml Technologies in Web Services," Journal on Soft Computing, vol. 3, no. 4, 2012.

[6] "Information technology — Security techniques — Information security management systems — Requirements," 2005.

[7] "www.iso.org," [Online].

[8] R. Bhanot and R. Hans, "A Review and Comparative Analysis of Various Encryption Algorithms," International Journal of Security and Its Applications, 2015.

[9] P. Mahajan and A. Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security," Global Journal of Computer Science and Technology Network, Web & Security, 2013.

[10] A. A. Hasib and A. A. Haque, "A comparative study of the performance and security issues of AES and RSA cryptography," in Proceedings. -3rd International.Conference. Convergence. Hybrid Information. Technology, 2008.

[11] R. H. Rathod and C. Dhote, "Comparison of symmetric key encryption algorithms," International Journal of Research in Information Technology (IJRIT), 2014.

[12] R. R. S. A. A. L, "A method for obtaining Digital Signatures and Public Key cryptosystems," Communication of the ACM, 1983.

[13] S. Nisha and M. Farik, "RSA Public Key Cryptography Algorithm–A Review," International journal of scientific & technology research, 2017.

[14] T. Bala and Y. Kumar, "Asymmetric Algorithms and Symmetric Algorithms: A Review," International Conference on Advancements in Engineering and Technology.

[15] H. A. Hamad, "Xml based data exchange in the heterogenous Databases (XDEHD)," International Journal of Web & Semantic Technology, 2015.

[16] M. Arenas and L. Libkin, "XML Data Exchange: Consistency and Query Answering".

[17] C.-x. Zhang, Y.-x. Hu, G.-b. Zhang and S. Jin, "Data Exchange based on Web Services," International Journal of Computer Science and Network Security, 2006.

[18] P. Dinesh, P. J. Charles and S. BrittoRamesh, "Security Issues in Web Services," International Research Journal of Engineering and Technology, 2016.

[19] D. Harris, L. Khan, R. Paul and T. Bhavani, "Standards for secure data sharing across organizations," Dallas, 2007.

[20] R. Datt, N. N. Jani, R. Mishra and P. Ajay, "Data Exchange Model Using Web Service For Herogeneous Databases," International Journal Of Advanced Research In Engineering And Technology, vol. 6, no. 4, 2015.

[21] A. A. Chandio, D. Zhu, A. H. Sodhro and M. U. Syed, "An Implementation of Web Services for Inter-Connectivity of Information Systems," International Journal of Computing and Digital Systems, 2014.

[22] V. V. Tan, . D.-S. Yoo and M.-J. Yi, "Efficient Web Service Based Data Exchange for Control and Monitoring Systems," International Journal of Information Technology, 2008.

[23] M. Mwanza and J. Phiri, "Fraud detection on bulk tax data using business intelligence data mining tool: A case of Zambia revenue authority," International Journal of Advanced Research in Computer and Communication Engineering, vol. 5, no. 3, pp. 793-798, March 2016.

[24] J. Phiri and T. Zhao, "Identity Attributes Quantitative Analysis and the Development of a Metrics Model using Text Mining Techniques and Information Theory," Proceedings of IEEE International Conference on Information Theory and Information Security, pp. 390-393, 2010.