A Study on the Secure Business Web Service Based on ebXML

Dongil Shin[1], Dongkyoo Shin[1*], Baek-Ho Sung[1], and Jun-Hong Song[2]

[1]Department of Computer Science and Engineering, Sejong University
98, Kunja-Dong, Kwangjin-Ku, Seoul 143-747, Korea
{dshin, shindk, guardia}@gce.sejong.ac.kr
[2]Industrial Bank of Korea (IBK), 50, 2-ga Ulchi-ro, Chung-gu, Seoul, Korea
lovelysong@ibk.co.kr

Abstract. While there is tremendous e-business value in the ebXML (Electronic Business using eXtensible Markup Language), security remains an unsolved problem and one of the largest barriers to adoption. XML Security technologies that have been emerging recently have extensibility and flexibility that is suitable for security implementation such as encryption, digital signature, access control and authentication. In this paper, we propose secure business Web Service models based on ebXML that allow trading partners to securely exchange XML based business transactions by employing XML security technologies.

1 Introduction

XML Security technologies emerging recently have extensibility and flexibility suitable for security implementation such as encryption, digital signature, access control and authentication. They are recommended to be used in ebXML security implementations. XML security technologies such as XML digital signatures [2] and SAML (Security Assertion Markup Language) [4] can be exploited to solve this problem. XML Encryption [1] is also recommended to solve the loss of confidentiality problem. Also, XKMS (XML Key Management Specification) [3] is recommended by the ebXML security team for key management as a substitute for PKI. In this paper, we propose secure business Web Service models based on ebXML that allow trading partners to securely exchange XML based business transactions by employing XML security technologies.

2 Secure Business Web Services Model Based on ebXML

We propose two ebXML business scenarios ensuring the trust relationship within the real trading partners. The first scenario performs a user authentication and updates the CPP in the repository. The procedure for the first scenario is presented in the form of

[*] Correspondence author

N. Koch, P. Fraternali, and M. Wirsing (Eds.): ICWE 2004, LNCS 3140, pp. 575–576, 2004.

a sequence diagram in Figure 1, where each box in the diagram denotes a Web Service or an application program. The second scenario performs business transactions within the trading partners, where security requirements are satisfied by applying security modules to implement business processes, as shown in Figure 2. In these scenarios, each XML security is constructed as a Web Service, which follows the Web Services standards proposed by the W3C and OASIS [1,2,3,4].

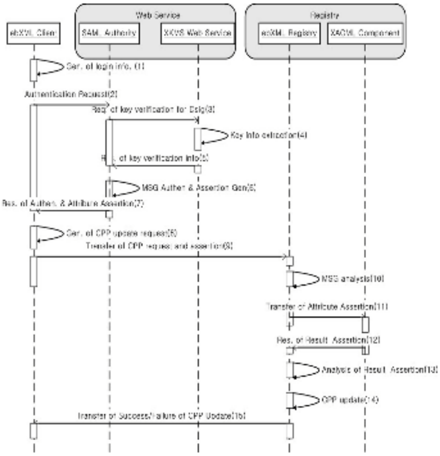
Web Service
Registry
ebXML Client
SAML Authority
XKMS Web Service
ebXML Registry
XACML Component
Gen. of login info. (1)
Authentication Request(2)
Req. of key verification for Dsig(3)
Key Info extraction(4)
Res. of key verification info(5)
MSG Authen & Assertion Gen(6)
Res. of Authen. & Attribute Assertion(7)
Gen. of CPP update request(8)
Transfer of CPP request and assertion(9)
MSG analysis(10)
Transfer of Attribute Assertion(11)
Res. of Result Assertion(12)
Analysis of Result Assertion(13)
CPP update(14)
Transfer of Success/Failure of CPP Update(15)

Fig. 1. Sequence Diagram – Senario 1

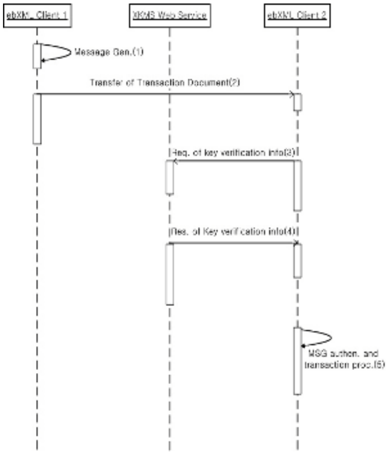
ebXML Client 1
XKMS Web Service
ebXML Client 2
Message Gen.(1)
Transfer of Transaction Document(2)
Req. of key verification info(3)
Res. of Key verification info(4)
MSG authen. and transaction proc.(5)

Fig. 2. Sequence Diagram – Senario 2

3 Design and Implementation of the Test Software

We constructed a test software, which focuses on security for registry/repository and messaging, and then targets system performance for the two business scenarios under a secure and reliable environment. XML Signature and XML Encryption are applied to the business transactions in the MSH (Message Service Handler) of ebXML client applications, registry, XKMS and SAML Web Services. We tested two scenarios by analyzing the messages in each step from Figure 1 and 2.

References

1. Imamura T., Dillaway B., Simon E.: XML Encryption Syntax and Processing, W3C Recommendation (2002), http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/
2. Bartel M., Boyer J., Fox B., LaMacchia B. and Simon E.: XML Signature Syntax and Processing, W3C Recommendation (2002), http://www.w3.org/TR/xmldsig-core/
3. Ford W., Baker H., Fox B., Dillaway B., LaMacchia B., Epstein J. and Lapp J.: XML Key Management Specification (XKMS) Version 2.0, W3C Working Draft (2003), http://www.w3.org/TR/2003/WD-xkms2-20030418/
4. Maler E., Mishra P., Philpott R.: Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1, OASIS Committee Specification (2003) http://www.oasis-open.org/committees/download.php/3406/oasis-sstc-saml-core-1.1.pdf