Conference Proceeding Issue Published in International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, www.ijtrd.com

Wireless XML Digital Signature on Heterogeneous Environment

[1]Jae Won Park, [2]Byambasuren Temuujin and [3]Eui In Choi,
[1,2,3]Department of Computer Engineering, Hannam University, Korea

Abstract: As wireless network was developed and increased, E-Commerce was activates in network environment. User authentication and security in E-Commerce environment is very important, so authentication technology, such as WPKI and XML digital signature in various network is studying. But WPKI is difficult to implement the heterogeneous system, it's not support XML digital Signature. Hermes system also not interoperate with XML digital signature system. So we proposed WXDS that can interoperate among digital signature systems and XML document to apply XML digital signature technology on heterogeneous system. Through system that suggested by us can supply XML digital signature on heterogeneous system.

Keywords: *Wireless; Heterogeneous system; User Authentication; WXDS; XML Digital Signature;*

I. INTRODUCTION

Today, E-Commerce was move to M-Commerce due to develop the wireless internet environment which was not connect physical network and performance of wireless terminal with mobility and portability.

Authentication in the E-Commerce was regard as important problem because it was related to security. So there was study that identified user to use digital signature by certificate published from the CA(Certification Authority). Recently, it is studying xml digital signature in authentication area. So we propose the digital signature technique that identified user when happened E-Commerce in heterogeneous system. Authentication techniques that are studied in wireless network was WPKI and Hermes system. But because there are many problem that wireless internet was very limitation on network environment then wire internet, process of authentication was very difficulty. So Java card technology that was able to compute the encryption and authentication value in wireless network was studied. Also WPKI was consisted of Heterogeneous system such as CA, content provider, authentication system based WPKI was very difficult to implement. Hermes system was used to XML document in E-Commerce, but because it was not use to XML digital signature technology, it was not interoperate XML digital signature system in wire internet.

In this paper, we implement WXML(Wireless XML Digital Signature) that process to compute digital signature value and other computation was process in mediator to make up for WPKI and Hermes weaknessand it was based Java card.

Our proposed system was expand XML digital signature technology that was able to sign in heterogeneous system. Also we can easily developed digital system in spite of heterogeneous environment that was consisted authentication, mobile cooperation, finance and can interoperate other digital signature systems.

II. RELATED WORKS

Research of user authentication in wireless environment was WPKI and Hermes System. It was studied user authentication based PKI in wire internet and XML digital signature technology is studying in proportion to actively process study of E-commerce using XML document.

A. WPKI

User of wireless internet was registered and published certificate by CA for communication of security to contents provider or to sign transaction. And then user was sign E-commerce document using private key store in wireless device through the certificate. The signed document was transport to web server through the WAP gateway, it was delivery CA, finally validate the signed document.

B. Hermes System

Hermes system was implemented to process user authentication to use digital signature in wireless internet. Hermes system was follow:

- User send service request to contents provider.
- Contents provider was received service request of user,and then send E-Commerce XML document to Hermessystem.
- After received XML document from Contents provider,Request receiver was check form of XML document use to XML parser. And then front end communicator was created message to sign, send it to wireless device. Created message was included contents of service, number of transaction, create date of message, expiration date of message.
- The message that send to mobile phone was signed by signature front end module and signed message was send to Hermes system.
- After received signed message, verifier was validate signed message through the trust center, when finished process of validation, the signed message delivery to Financial-institute communicator to write new XML document.
- Financial-institute communicator that received signed document was create XML document that included initial request of contents provider, user request, transaction, account number, and it was send to

financial-institute with signed message

- Financial-institute was validate the XML document and signed message.
- Concluded service was send to verifier form of receipt, and verifier was validate it through trust center.

III. PROPOSED WXML DIGITAL SIGNATURE

A. Design of WXML

Wireless internet had limitation, such a narrow bandwidth, worst powerful CPU, small memory capacity, small store capacity, small display device. There are difficulty that process the XML digital sign in wireless device such a limitation. So our system was design module that compute the digital signature value in heterogeneous(mobile) device and mediator separately. Figure 1 was WXML system that we were suggested WXML was consisted follows :

Mobile phone

It was used when user buy the product or use the service, and compute the signature value for digital signed in user authentication.

Content provider

Supply the contents and service in wire internet and communicate with user.

WXML mediator

Create the element of XML digital document in E-Commerce and send canonicalization value of sign info to mobile phone. Finally, received the signature value and other information from mobile device and create the XML digital signature document use to it

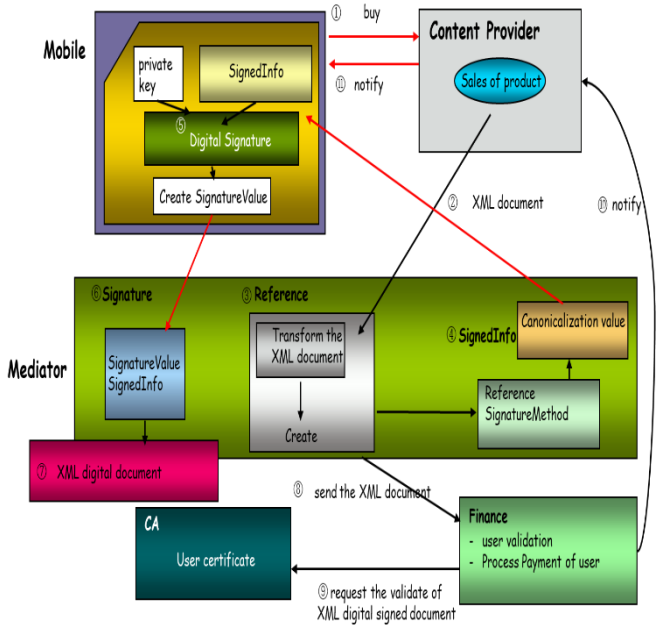

Fig. 1 WXML

CA (Certification Authority)

Published the certificate to user, provide the information(public key, certificate information) for validate the signed document.

Finance

Provide the finance service for trade between user and contents provider, validate document that signed by user. After conclude process of payment, notified payment complete to contents provider.

B. XML message code

Figure 2 is example of XML digital signature document that used WXML. Because performance of mobile device was the lowest then wireless device, it was difficult that XML digital signature document. So it was send only digest value(E6lwx3RvEPS0vKtMep4NbeVu8nk) to mobile device for compute signature value in <SignatureValue> element. In our system, such a digest value transforms to signature value(……....) by using API of Java card.

```
<?xml version="1.0" encoding="UTF-8"?>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
<SignedInfo Id="Example">
<CanonicalizationMethod
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315"/>
<SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1" />
<Reference URL>
<DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
<DigestValue>E6lwx3RvEPS0vKtMep4NbeVu8nk=</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>……....</SignatureValue>
</Signature>
```

Fig. 2 XML digital signature message code

IV. COMPARATIVE ANALYSIS AND CONCLUSION

Table 1: Analysis and compare with WXML and Hermes system

	Hermes system	WXML
object of signature	transaction	canonicalization value
integrated	using XML document	using XML document
interoperation	no	yes
expansion	need to transform	expanded easily
stability	good	-

Since there are not yet standard of WPKI, it was difficult that WPKI digital signature system implement in heterogeneous environment. Also in case of Hermes system, XML document was used in E-Commerce, it was not used XML digital signature technology, but signed to transaction. So it was not interoperate with XML digital signature system. But because our WXML system was used to XML digital signature technology, was able to interoperate with XML digital signature system, and easily integrate with other contents provider for using XML document.

As developed E-commerce in wireless internet, study of user authentication, such as Hermes system, XML digital signature technology and smart card for increasing for mobile device are progressing actively. To resolve this problem, we are design and implement the WXML system that could signed in heterogeneous environment. Also, because of limitation of mobile device, all process of XML digital signature was not

possible in mobile device. So WXML system was implement to compute digital signature value in Java card.

Our future work need to validate data security and stability of WXML.

References

[1] XML-Signature Syntax and Processing, W3C, 12 February 2002

[2] Aphrodite Tsalgatidou, "Mobile Electronic Commerce:Emerging Issues", Procs of EC-WEB 2000, pp.477-486

[3] WPKI(Wireless Public Key Infrastructure), Version 24 Apr 2001

[4] Henna Pietiläinen, "Elliptic curve cryptography on smart cards", Helsinki University of Technology, 2000

[5] R.L. Rivest, A.Shamir, L.Adleman, "A method for obtaining digital signatures and public key cryptosystems", ACM, 21(2), February 1978

[6] Patrice Peyret, 'Java CardTM Technology for Smart Cards : Architecture and Programmer's Guide', Addison Wesley

[7] Java CardTM 2.1.1 Development Kit User's Guide, Sun Microsystems

[8] Digital Signature Standard(DSS), U.S. Department of Commerce/National Institute of Standard and Technology, 2000 January 27

[9] Sebastian Fishmeister, "Hermes - A Lean M-Commerce Software Platform Utilizing Electronic Signatures", IEEE. Hawaii Internation Conference on system Sciences, January 7th 10, 2002

[10] Brokat. WWW Site. http://www.brokat.com

[11] Paybox. WWW Site. http://www.paybox.de

[12] SK Telecom, http://www.moneta.co.kr

[13] Thomas Weigold, “Java-Based Wireless Identity Module”, London Communications Symposium 2002