무선네트워크에서 XML 서명을 위한 WXDS 시스템 구현

김석훈*, 정두용**, 장창복***

요약

무선네트워크 환경의 성장과 무선 장비들의 성능이 향상됨에 따라서, 무선장치를 이용한 전자상거래가 활발히 이루어지고 있다. 따라서 많은 사용자들은 다양한 멀티미디어 데이터들을 무선 장치를 이용하여 다운로드하고 있다. 하지만 멀티미디어 데이터를 사용하기 위해서는 지불이 필요하고 이에 따라 사용자의 인증이 요구된다. 그러므로 WPKI, WPLS와 같은 사용자 인증 기술이 연구되어왔다. 하지만 이러한 인증기술 및 시스템들은 이질적인 환경에서 구현하기가 매우 어렵고, 인증 시스템들간에 상호작용하기가 어려우며, XML 전자서명 기법이 존재하지 않는다. 따라서 본 논문에서는 유선 및 무선 네트워크 환경에서 XML 전자서명을 적용하여 XML 문서를 사용하고, 전자서명 시스템간에 상호운용이 가능한 WXDS을 구현하였다. 제안된 시스템을 통하여 무선장치에서 XML 전자서명이 가능하며, 사용자들은 XML 전자서명을 통해 다양한 멀티미디어 데이터를 이용할 수 있다.

WXDS for XML Digital Signature on Wireless Network

Seok-Hun Kim*, Doo-Yong Jung**, Chang-Bok Jang***

ABSTRACT

As wireless network was grown and performance of wireless device was increased, M-Commerce was activates in Wireless network environment. Therefore many user downloaded various multimedia data(picture, movie, music) by use the wireless network. But for using the multimedia data, it need authentication of user for paying. So authentication technology, such as WPKI and WPLS, Hermes system, is studying. But if authentication systems was implemented to heterogeneous, system that used WPKI technology is difficult to implement, it's not interoperate with authentication system on wire internet, not support XML digital Signature. Hermes system also not interoperates with XML digital signature system. So our paper designed WXDS(Wireless XML Digital signature System) that can interoperate with other digital signature systems and use to XML document to apply XML digital signature technology on wire and wireless network, and then implemented system that can sign to XML digital signature by java card. Through system that suggested by us can supply XML digital signature on the mobile phone. And user can sign multimedia data whereas on wire network and mobile phone.

Key Words : Authentication, WPKI, XML Digital Signature, Wireless network

* (주)파라곤베이스
** 공주영상대학 공무원양성과
*** 한남대학교 컴퓨터공학과
· 제1저자(First Author) : 김석훈 · 교신저자(Correspondent Author) : 장창복
· 접수일(2010년 2월 19일), 수정일(1차 : 2010년 3월 22일), 게재확정일(2010년 3월 25일)

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. M-Commerce is form of E-Commerce that pay money to use wireless device such as Mobile phone when buys product or Digital contents in shopping mall. And authentication and data Security In the E-Commerce was regard as important problem because it was related to money. So there was study that identified user to use digital signature by certificate published from the CA(Certification Authority). Recently, because it is actively studying E-Commerce that used XML document in wire Internet environment, studying XML digital in user authentication field.[1, 4]. So we need the digital signature technology that identified user when happened E-Commerce in wireless network, such a wire network. Authentication Technology that studied in wireless network was WPKI in WAP Forum and Hermes System in Constance University of German[3, 9]. But Because there are many problem that Wireless internet was very limitation on wireless device performance and network environment then wire internet, Data encryption and 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 [5, 8, 10, 13]. Also WPKI was consisted of Heterogeneous system such as CA, Mobile Cooperation, Finance, 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.

So in our paper, we implement WXDS(Wireless XML Digital Signature) that process to compute digital signature value in wireless device and other computation was process in mediator to make up for WPKI and Hermes weaknees and it was based java card.

Our system was expanded XML digital signature technology that was able to sign in hetero-geneous system to wireless internet from wire internet. And it was able to efficient process of business task because of sign the XML document in wireless internet. 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

2.1 WPKI

WPKI was expand to PKI in wire internet for wireless internet and suggested in WAP Forum. 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 docu-ment 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.

2.2 Hermes system

Hermes system was implemented to process user authentication to use digital signature in wireless Internet. The goal of this project is to study software architectures for mobile computing in the context of services for mobile phones. This project has been a proxy-based software

architecture using asynchronous messaging . And there are some problem that the certification process is very complex and is not suitable for real world use [9].

① User send service request to contents provider.

② Contents provider was received service request of user, and then send E-Commerce XML document to Hermes system.

③ After received XML document from Contents provider, Request receiver was check form of XML document use to XML parser. And then frontendcommunicator 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.

④ The message that send to Mobile Phone was signed by Signature Front End mod-ule and signed message was send to Hermes system.

⑤ 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.

⑥ 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

⑦ Financial-institute was validate the XML document and signed message.

⑧ Concluded service was send to verifier form of receipt, and Verifier was validate it through Trust Center.

III. WXDS System

3.1 Design of WXDS based java Card for XML digital signature

Wireless internet had limitation, such a narrow bandwidth, worst powerful CPU, small memory capacity, small store capacity, small display device. there are very 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 wireless device and WXDS mediator separately. Figure 1 shows structure of WXDS system that we were suggested.

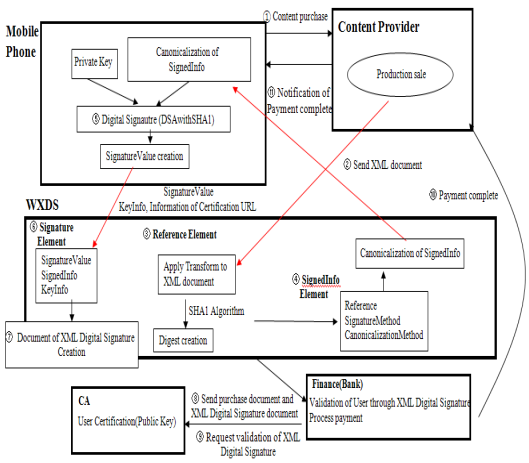

그림 1. WXDS의 구조
Fig. 1. Structure of WXDS

WXDS was consisted of Mobile phone, Content provider, WXDS, CA, Finance.

① Mobile phone(Wireless Device) : It was used when user buy the product or use the service, and compute the Signaturevalue for digital signed in user authentication.

② Content Provider : supply the contents(multimedia data) and service in wire internet and communicate with user.

③ WXDS : Create the element of XML digital document in E-Commerce and send Canoni-calization value of SignInfo to Mobile phone. Finally, received the SignatureValue and other information from mobile phone and create the XML digital Signature document use to it

④ CA(Certification Authority) : Published the certificate to user, provide the information (public key, certificate information) for validate the signed document.

⑤ 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.

3.2 Algorithm of digital signature in WXDS

① Application of digital signature

In WXDS, digital signature was process to send canonicalization value of SignInfo that created from WXDS mediator to mobile phone, and create the r, s value of signature that using private key. And then r, s value which was created send to WXDS mediator. In our paper, we used to DSA(Digital Signature Algorithm) for digital signature algorithm. And we implements code that computes r, s value to use the Java card API. Table 1 shows variable and function for application of digital signature which we used in application. The codes, which compute the r, s value, are the following:

```
BigInteger Sign_Result_R = G.modPow(k, P).mod(Q);
BigInteger Private_key_R_Plus_h
 = Sign_Result_R.multiply(private_key).add(h);
BigInteger Sign_Result_S
= k_inverse.multiply(Private_key_R_Plus_h).mod(Q);
```

② verify Application

In our paper, we use also DSA algorithm and implements code that verify to r, s value by used java card API, such as following code :

```
BigInteger W = Sign_Result_SS.modInverse(QQ);
BigInteger u1 = Verify_hash.multiply(W).mod(QQ);
BigInteger u2 =
Sign_Result_RR.multiply(W).mod(QQ);
BigInteger v1 = GG.modPow(u1, PP);
BigInteger v2 = public_key.modPow(u2, PP);
BigInteger v = v1.multiply(v2).mod(PP).mod(QQ);
```

3.3 WXDS Signature Process

Signature process of WXDS that suggested follows:

① User send service request to contents provider.

② Contents provider was received service request of user, and then send E-Commerce XML document to WXDS system.

③ After received XML document from Contents provider, WXDS was check form of XML document use to XML parser. And then creates reference element and SingInfo element. After compute canonicalization value of SignInfo element, send it to wireless Device.

④ The message that send to Mobile Phone was signed with private key and create Signaturevlaue, and then was send it to WXDS system.

⑤ After received Signaturevalue, WXDS creates Signature element. Finally it made XML document that consist of Reference, SignInfo, Signature element. For validating signed message in the Trust Center and completing payment process, WXDS send signed XML document to Financial-institute.

⑥ Financial-institute that received signed XML document was send it to CA to validate au-thentication of user.

⑦ CA was validate the signed XML document and send result of it to Financial-institute.

⑧ Financial-institute was complete payment service according to result, send it to contents provider.

3.4 XML message code

Figure 2 is example of XML digitalsignature document that used WXDS. Because performance of wireless device was the lowest then wire device, it was difficult to create XML digital signature document directly. So we weresend only digest value (E6lwx3RvEPS0vKtMep4NbeVu8nk) to wireless device for compute signature value in <SignatureValue> element. In our system, such a digest value transforms to signature value(79738777230...) 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/xmldsi
g#dsa-sha1" />
<Reference URI="http://larkspur.hannam.ac.kr/example.htm">
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
<DigestValue>E6lwx3RvEPS0vKtMep4NbeVu8nk=</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>79738777230...</SignatureValue>
</Signature>
```

그림 2. XML 문서
Fig. 2. XML message code

Ⅳ. Analysis and Compare

Table 3 is analysis and comparison WXDS with WPKI and Hermes system.

표 2. WXDS와 다른 시스템과의 비교
Table 2. Analysis and compare with WPKI and Hermes system

	WPKI	Hermes	WXDS
Signature	Transaction	Transaction (Message)	Canonicalization value of SignedInfo
Integration	difficulty	easy (XML document)	easy (XML document)
Interoperation	No	No	Yes
Implementation and expansion	difficulty	Need to transform of Component(module)	easy

To implement Digital signature system in WPKI, need to interoperate with CA, Contents provider, Finance, Wireless device provider, Telecommunicate Cooperation. Since there are not yet standard of WPKI, it was difficult that WPKI digital signature system implement in heterogeneous environment [3]. 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(message). So it was not interoperate with XML digital signature system[9]. But because our WXDS 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.

Ⅴ. Conclusion

Today, as developed E-commerce in wire and wireless internet, many users download various multimedia data, therefore it need the authentication technology. So, study of user authentication, such as WPKI, Hermes system, PKI, XML digital signature technology and smart card for performance increasing of wireless device are progressing actively. But WPKI system was difficult that system

implement in case of consisting with heterogeneous system, Hermes system also was not interoperate with XML digital signature system. And because wire and wireless authentication technology is not yet compatible each other, should implement different digital signature system in wire and wireless environment.

So, to resolve this problem, we are design and implement the WXDS system that could signed in wire and wireless environment. Also, because of limitation of wireless device, all process of XML digital signature was not possible in wireless device. So WXDS system was implemented to compute digital signature value in java card. WXDS system was able to interoperate with wire XML digital signature system and sign by using Method of the XML digital signature in wireless Internet.

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

[14] 황문영 외, "클라우드 컴퓨팅 환경에 적합한 사용자 중심의 ID 관리기술", *한국지식정보기술학회 논문지*, 제5권 제1호, pp.51-58, 2010.

김석훈(Seok-Hun Kim)

2003년 한남대학교 컴퓨터공학과 (공학석사)
2006년 한남대학교 컴퓨터공학과 (공학박사)
2007년~현재 (주)파라곤베이스 기술이사
※ 관심분야 : 웹 DB, 네트워크, VoIP, 모바일컴퓨팅

정두용(Doo-Yong Jung)

서강대학교 전자계산학과(이학석사)
경희대학교 전자계산공학과 박사수료
1999년~현재 공주영상대학 공무원양성과 교수
※ 관심분야 : 유비쿼터스, 실시간 운영체제, USN

장창복(Chang-Bok Jang)

2003년 한남대학교 컴퓨터공학과 (공학석사)
2007년 한남대학교 컴퓨터공학과 (공학박사)
2009년~현재 한남대학교 컴퓨터공학과 BK21 연구교수
※ 관심분야 : 데이터베이스, 유비쿼터스, 네트워크