Security Certification Model for Mobile-Commerce

Haeng-Kon Kim

Abstract. The most important technology in the mobile commerce based on mobile applications is to guarantee the certification and security of trading information exchange. Many technologies are proposed as a standard to support this security problem. M(Mobile)-commerce is a new area arising from the marriage of electronic commerce with emerging mobile and pervasive computing technology. The newness of this area and the rapidness with which it is emerging makes it difficult to analyze the technological problems that m-commerce introduces and, in particular, the security and privacy issues. This situation is not good, since history has shown that security is very difficult to retro-fit into deployed technology, and pervasive m-commerce promises to permeate and transform even more aspects of life than e-commerce and the Internet has. One of them is an XML (eXtensible Markup Language). This is used in various applications as the document standard for electronic commerce system. The XML security has become very important topic. In this paper, we propose the XML security model for mobile commerce services based electronic commerce system to guarantee the secure exchange of trading information. To accomplish the security of XML, the differences of XML signature, XML encryption and XML key management scheme respect to the conventional system should be provided. The new architecture is proposed based on unique characteristics of mobile commerce on XML. Especially the method to integrate the process management system need to the electronic commerce is proposed.

Keywords: Mobile commerce, Mobile security, XML management, Mobile, networks.

Haeng-Kon Kim
School of Information Technology, Catholic University of Deagu, Korea
e-mail: hangkon@cu.ac.kr

R. Lee (Ed.): *SERA*, SCI 496, pp. 1–15.
DOI: 10.1007/978-3-319-00948-3_1

1 Introduction

Mobile commerce is an interesting and challenging area of research and development. It presents many issues that cover many disciplines and may best be addressed by an active participation of computer and telecommunications experts, social scientists, economists and business strategists. M-commerce introduced several new classes of applications, reviewed networking requirements, and discussed application development support. Since the area of mobile commerce is very new and still emerging, several interesting research problems are currently being addressed or should be addressed by the research and development community. It is believed that user trust will play a crucial role in acceptance and widespread deployment of mobile commerce applications. Regarding m-payment, some systems are under development or already operational. One of the main future challenges will be to unify payment solutions, providing the highest possible level of security.

Much of information is propagated by Internet. Internet that is an open communication system provides browsers based on easy protocols and various tools for information handling. Therefore m-commerce is proliferated. This m-Commerce is based on the standards for document processing in Internet

In the last few years, advances in and widespread deployment of information technology have triggered rapid progress in m-commerce. This includes automation of traditional commercial transactions (electronic retailing, etc.) as well as the creation of new transaction paradigms that were infeasible without the means of widely deployed information technology. New paradigms include electronic auctioning of purchase orders, as well as novel, with less transaction models such as Napster [1]. M-commerce has heightened the focus on security both of systems and also for messaging and transactions [2].

The enterprises perform not only the internal activities but also the interactive businesses with other companies to secure the competitive power of them. In general, the trading business between enterprises is performed typically according to the pre-defined business process by exchanging the contracted documents.

The purpose of this paper is to propose a business model for B2B environment for m-commerce. This model is based on the business process management system which manages the conventional internal processes of enterprises. This model also analyzes the key elements needed to m-commerce for inter-enterprises. Especially, the documents and data exchanged between companies is formalized by using the XML messages that are approved as the standard tools for information exchanges. The business processes exchange the XML messages. During all processes, therefore, the efficient business integration may be possible. This model ensures the secure information exchange which is an essential factor in m-commerce as in figure 1.

The m-commerce should be based on the public key encryption system to authenticate the valid users. The method to ensure the reliability and security of user's public keys is required. Public key infrastructure (PKI)

provides secure and reliable method to open the user's public keys to the public [3]. Public key infrastructure has very important roles in Internet E-Commerce. It opens the user's public keys to public in secure and reliable manner. Since the XML technology is used as the format of message exchange in Internet e-Business, the security for XML documents becoming essential and XML digital signature should be supported for secure m-commerce [4,5].

In this paper, the security application of m-commerce is designed which is reliable by using X.509 certificate based on PKI. A web service is designed to implement the PKI-based security application for mutual authentication. The digital signature protocol based on PKI and XML is also designed to solve the security and repudiation problem of message exchange in B2B on m-commerce.

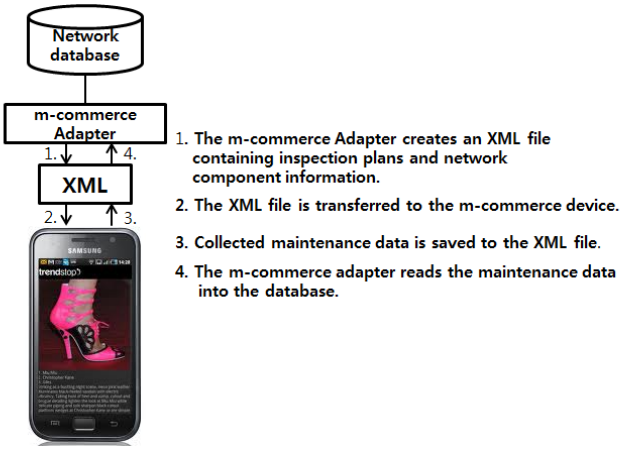

Fig. 1 Secure Information Exchange in M- Commerce

2 Background Study

2.1 Security for Mobile Commerce Applications

Security for mobile Commerce application is a crucial issue. Without secure commercial information exchange and safe electronic financial transactions over mobile networks, neither service providers nor potential customers will trust mobile commerce systems. From a technical point of view, mobile commerce over wireless networks is inherently insecure compared to electronic commerce over the Internet. The reasons are as follows:

- Reliability and integrity: Interference and fading make the wireless channel error-prone. Frequent handoffs and disconnections also degrade the security services.

- Confidentiality/privacy: The broadcast nature of the radio channel makes it easier to tap. Thus, communication can be intercepted and interpreted without difficulty if no security mechanisms such as cryptographic encryption are employed.
- Identification and authentication: The mobility of wireless devices introduces an additional difficulty in identifying and authenticating mobile terminals.
- Capability: Wireless devices usually have limited computation capability, memory size, communication bandwidth and battery power. This will make it difficult to utilize high-level security schemes such as 256-bit encryption.

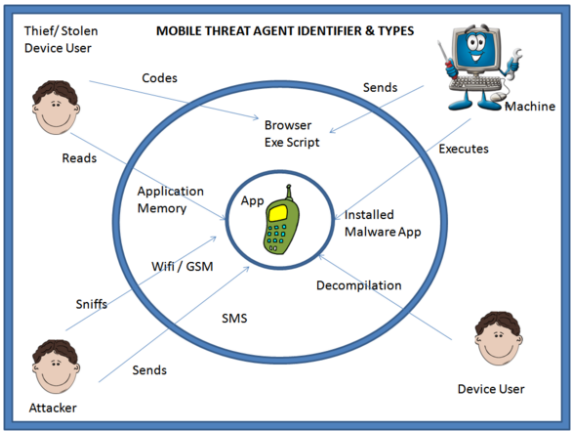

Fig. 2 Securities Mechanisms and Systems

Mobile commerce security is tightly coupled with network security. The security issues span the whole mobile commerce system, from one end to the other, from the top to the bottom network protocol stack, from machines to humans. Therefore, many securities mechanisms and systems used in the mobile application and commerce may be involved as in figure 2.

Public key encryption system is an asymmetric system which is based on mathematical functions. It has the pair of keys one is opened to public and the other is saved securely instead of private key encryption system. Then the key is opened is called public key, the other is called private key. The majority security systems for E-Commerce based on public key algorithm because the key management and distribution are difficult. It also resolves the anonymous and user authentication problems.

Public key infrastructure should be constructed based on public key certificates. The certification authority(CA) authenticates the trading subjects. The certification authority creates digital signature by using their own private key and attaches them to the certificate for proving the subject users

are valid. The certificate includes the public key of certificate's users and information of subject users.

2.2 M-Commerce Framework

This emerging area of m-commerce creates new security and privacy challenges because of new technology, novel applications, and increased pervasiveness. Mobile applications will differ from standard e-commerce applications, because the underlying technology has fundamental differences:

- **Limitations of Client Devices.** Current (and looming) PDAs are limited in memory, computational power, cryptographic ability, and (for the time being) human I/O. As a consequence, the user cannot carry his entire state along with him, cannot carry out sophisticated cryptographic protocols, and cannot engage in rich GUI interaction.
- **Portability of Client Device.** PDAs have the potential to accompany users on all activity, even traditionally offline actions away from the desk-top. Besides creating the potential for broader permeation of e-transactions, this fact also makes theft, loss, and damage of client devices much more likely.
- **Hidden and Unconscious Computing.** Both to compensate for limited PDA storage, as well as to provide new ways to adapt a user's computing environment to her current physical environment, pervasive computing often permits client devices to transparently interact with the infrastructure without the user's direct interaction. This unconscious interaction can include downloading executable content.
- **Location Aware Devices.** When the user is mobile, the infrastructure can potentially be aware of the location of the user (e.g., in a particular telephone cell). This knowledge introduces a wide range of applications which have no analogue in the stationary user model.
- **Merchant Machines.** In the e-commerce world, the merchant (i.e., the party that is not the user) has powerful machines, with ample storage and computation, usually in a physically safe place. However, to fully exploit the potential interacting with mobile, PDA equipped users, merchant machines may move out into the physical world. This move brings with its own challenges of increased physical exposure, limited computation and state, and limited interconnection.

The most threatened factor to the m-commerce is the security problems. The messages exchanged by an XML message via Internet is not secure because the user authentication is not guaranteed as shown in Fig. 3 [6].

We are aware that consensus within business and industry of future applications is still in its infancy. However, we are interested in examining those future applications and technologies that will form the next frontier of electronic commerce. To help future applications and to allow designers,

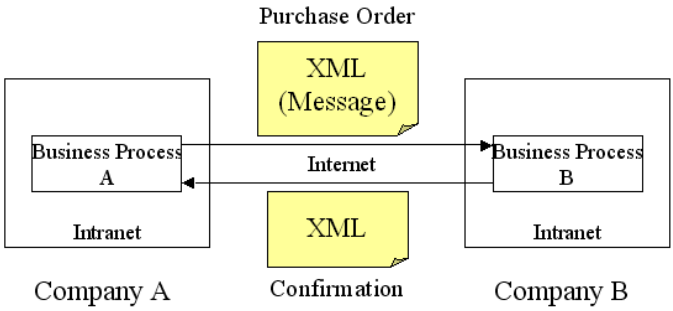

Fig. 3 Unsecured message exchange

developers and researchers to strategize and create mobile commerce applications, a four level integrated framework is proposed as in figure 4.

These four levels are as follows: m-commerce applications, user infrastructure, middleware and network infrastructure which simplifies the design and development. By following this framework a single entity is not forced to do everything to build m-commerce systems, rather they can build on the functionalities provided by others. The framework also provides a developer and provider plane to address the different needs and roles of application developers, content providers and service providers.

Service providers can also act as content aggregators, but are unlikely to act as either an application or content provider due to their focus on the network and service aspects of m-commerce. Content provider can build its service using applications from multiple application developers and also can aggregate content from other content providers and can supply the aggregated content to a network operator or service provider.

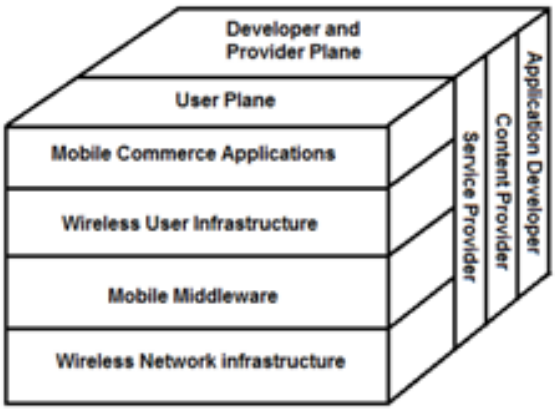

Fig. 4 Framework of M-commerce

2.3 Mobile Applications and XML

M-commerec services are software interface which can be found and called by another programs on the web regardless of location and platforms. M-commerec service is independent on platforms, devices and location. M-commerec service provides dynamic functionality. M-commerec service can be also applied to the conventional systems by low cost. The mobile applications service in m-commerce is a standardized software technology which combines conventional computer system programs between businesses on Internet. This standard technology enables all business functionalities and services. The M-commerec services by using Internet overcome the differences of communications among the heterogeneous operation systems and programming languages. So to speak, the web services are software components which conform e-Business standard and have business logics of Internet. XML standard describes the classes of data objects for XML documents. It also describe the operations of computer programs which process these XML documents. XML is an application of SGML (Standard Generalized Markup Language).

XML documents consist of entities which are storage units. The entity contains parsed data or un-parsed data. The parsed data consists of characters. Some of these characters are character data, the others are markups. The markups encode the arrangement plan of physical storage and the description of logical structure. XML provides a mechanism which enforces the arrangement plan of storage and logical structure. The software module as it called XML processor reads XML document and accesses the content and structure of that. XML is a standard for organizing the data, XSL (eXtensible Stylesheet Language) is a standard for method to output this data. XSL is a translation technology. XSL is a language to translate each field of XML to relevant tags of HTML and represent to web browser. XML schema is the term for file to define the structure and content of XML documents. DTD (Document Type Definition) is also a kind of schema, but it has some defects. DTD should be described by E-BNF and so difficult. On the other hand, XML schema can be desctibed just using XML itself. Moreover, XML schema can use various data types that are not supported in DTD. In XML schema the elements can be reused. So to peak, XML schema extended model of DTD. XML schema can define precisely the types of XML documents and the relationships of elements. XML documents should be parsed to make a tree structure from XML elements. DOM (Document Object Model) is a model to store parsed data as a tree structure and permits accessing particular element. According to DOM, XML documents are analyzed to client and server structure as in figure 5.

Recently, XML is in the spotlight as a technology applicable to various applications like B2B and B2C. The importance of security is increased in E-Commerce because the most businesses are processed in electronically. Especially, the standards for security in documents exchanging using XML in m-commerce have been established. The XML-Signature Group of IETF and

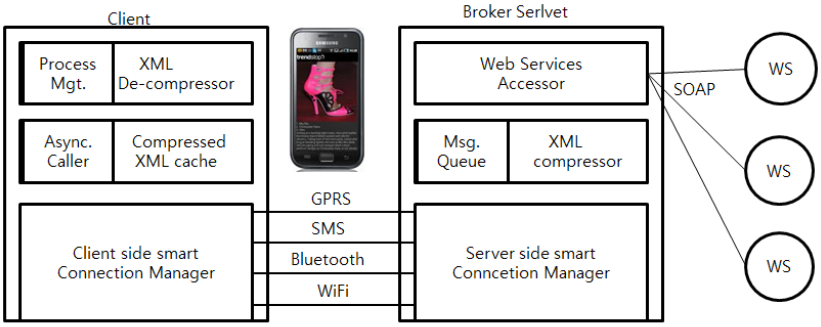

Fig. 5 Client-Server Structure for M-commerce on XML

W3C recommended the specification for "XML-Signature Syntax and Processing". This specification describes the syntax and processes for XML digital signature.

The following should be considered for security of XML digital signature.

- Confidentiality
- Integrity
- Authentication
- Authorization
- Non-Repudiation

3 Mobile Commerce Security Model

3.1 M-Commerce Security Issues

As mentioned earlier, m-commerce is not possible without a secure environment, especially for those transactions involving monetary value. Depending on the point of views of the different participants in an m-commerce scenario, there are different security challenges . These security challenges relate to:

- **The mobile device -** Confidential user data on the mobile device as well as the device itself should be protected from unauthorized use. The security mechanisms employed here include user authentication (e.g. PIN or password authentication), secure storage of confidential data (e.g. SIM card in mobile phones) and security of the operating system.
- **The network operator infrastructure -** Security mechanisms for the end user often terminate in the access network. This raises questions regarding the security of the users data within and beyond the access network. Moreover, the user receives certain services for which he/she has to pay. This often involves the network operator and he/she will want to be assured about correct charging and billing.

- **The kind of m-commerce application -** M-commerce applications, especially those involving payment, need to be secured to assure customers, merchants, and network operators. For example, in a payment scenario both sides will want to authenticate each other before committing to a payment. Also, the customer will want assurance about the delivery of goods or services. In addition to the authenticity, confidentiality and integrity of sent payment information, non-repudiation is important.

The figure 6 shows the security issues for m-commerce in the view of stakeholders as application developers, contents provider, wireless service provider, equipment vendors and other service provider in this paper.

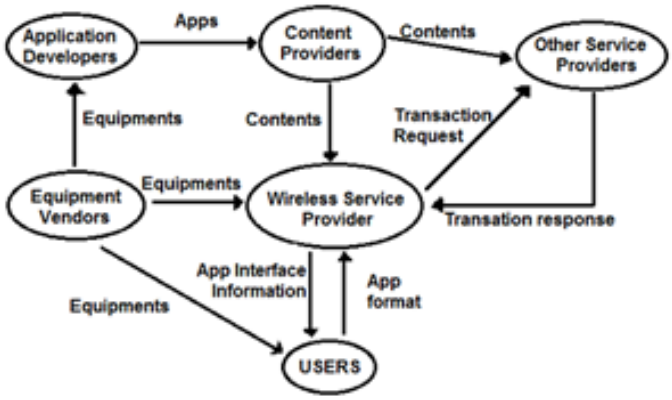

Fig. 6 M-commerce Security Issues

3.2 Mobile Applications Signature

The syntax of XML signature is a complicated standard to provide various functionalities. It can be applied any signatures because it is designed to have high-level extensibility and flexibility. W3C recommendation defined XML signature syntax and processing rules for them. Traditionally, middleware unites different applications, tools, networks and technologies; allowing user access via a common interface. Mobile middle-ware can be defined as an enabling layer of software that is used by the applications development to connect the m-commerce applications with different networks and operating systems without introducing mobility awareness in the applications. To allow for web content to be accessible from everywhere, from PCs to TVs to palm devices to cellular phones, the World Wide Web consortium (W3C) had developed several recommendations. These recommendations include the Extensible Makeup Language (XML) for richer semantic information, improved Cascading Style Sheets (CSS) and Extensible Style Sheet Language (XSL) to

further separate content from presentation, and a Document Object Model (DOM) which defines a language independent application programming interface that applications can use to access and modify the structure, content and style of HTML and XML documents. Fig.7 shows the Mobile middleware for Certification Model for Mobile-Commerce [7].

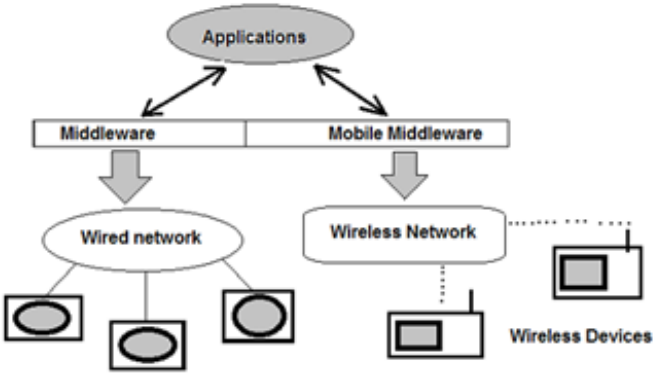

Fig. 7 Mobile middleware Certification Model for Mobile-Commerce in this paper

XML signature starts with an element <Signature>. The element <Signature>is an important one that consists of signature and identifying the signatures. The element <SignedInfo>lists "the signed information" which are the objects to sign by us. The particular data streams for Digest is represented by the element <References>. The URI (Uniform Resource Identifier) syntax is used to prescribe these streams. The element <KeyInfo>may be used efficiently in automation of XML signature processing because it provides identifying mechanism for verification keys. The element <Object>is a container which can retain any types of data objects. Two elements for <SignatureProperties>and <Manifest>are defined that should be contained in the element <Object>. The element <SignatureProperties>is a pre-defined container to verify signatures. It retains the assertions for signatures. These assertions may be used to verify the signatures and integrity. The element <Manifest>is used to verify references for application domains. It also provide a convenient method for multiple-signers to sign multiple documents. If the element <Manifest>does not used, the results of signature increase in volume and the performance may be depreciated. The creation information for certificates and the issued certificates are exchanged in the form of XML documents. The important information is encrypted as a unit of XML element.

3.3 Structure for XML Security

In this paper, the security system is designed based on the web service platform. This system executes and verifies XML signatures independent from the conventional applications. Consider the Purchase Order is submitted by Company A via Internet and is confirmed by Company B as shown in Fig. 7. Company A executes digital signature before transmission and Company B confirms after reception. So, the secure SOAP message exchanges are possible. In this process the Proxy has a role to check the digital signatures under surveillance of delivered messages. The real object to execute and to confirm the digital signature is implemented as a web service. The following is the procedures for. Mobile Secure exchange of XML messages as in figure 8.

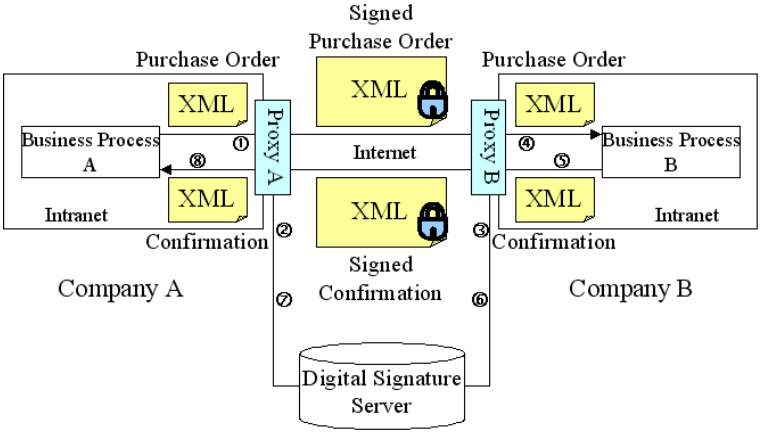

Fig. 8 Mobile Secure exchange of XML messages

Step 1. The business process A of company A transmits the message for Purchase Order to business process B of company B.

Step 2. When the purchase is passing proxy A, the digital signature is executed by sending the message to digital signature server.

Step 3. The proxy B of company B receives the signed message and sends it to the confirmation server. The confirmation server verifies the signed message.

Step 4. The verification results are sent to proxy B. If the signature is valid, proxy B removes the signature and sends it to business process B. The information of signer may be preserved.

Step 5. The business process B transacts the message for Purchase Order. The business process B makes a reply message and transmits it to company A.

Step 6. When the reply message is passing proxy B, the digital signature is executed using the private key of company B by sending the message to digital signature server.
Step 7. The company A sends the message from Proxy A to the confirmation server.
Step 8. If the digital signature is valid, the signature is removed from the message and the message is sent to the business process A.

The proxy determines whether it executes digital signature or not by checking the XML messages on network. Consequently, the workflow A and B do not concern the execution and confirmation of signatures. It is a forte that the conventional applications may not be changed.

The content verifier of the proxy server determines whether it needs a digital signature or not by checking the existence of an element <Signature>in XML schema. If it needs, two modules are required. One is to translate the XML message to the form of SOAP message, the other is reverse.

3.4 Execution of Digital Signature

Figure 7 shows an example of the message for Purchase Order with digital signature. The procedure to execute the message in Fig. 9. by digital signature web service is as follows:

Step 1. Determine the object for digital signature. This is given as the form of URI in general.
Step 2. Calculate the value of Digest for each object for signature. The object for signature is defined in the element <Reference>and each

```
<?xml version="1.0" encoding="UTF-8"?>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
<SignedInfo Id="foobar">
<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1" />
<Reference URI="http://www.acompany.com/news/2000_03_27_00.htm">
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
<DigestValue>j6lwx3rvEPO0vKtMup4NbeVu8nk=</DigestValue></Reference>
<Reference URI="http://www.w3.org/TR/2000/WD-xmldsig-core-20000228/signature-sample.xml">
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>UrXLDLBIta6skoV5/A8Q38GEw44=</DigestValue></Reference>
</SignedInfo>
<SignatureValue>MC0E-LE=</SignatureValue>
<KeyInfo>
<X509Data>
<X509SubjectName>CN=Ed Simon, O=XML Security Inc., ST=OTTAWA, C=CA</X509SubjectName>
<X509Certificate> MIID5jCCA0+gA...1VN </X509Certificate>
</X509Data>
</KeyInfo>
</Signature>
```

Fig. 9 XML Digital Signature

Digest is stored in the element <DigestValue>. The element <DigestMethod>defines the algorithm.

Step 3. The element <SignedInfo>contains the elements <Reference>of each objects for signature. The element <CanonicalizationMethod> designates the algorithm that normalizes the element <SignedInfo>.

Step 4. The Digest of the elements <SignedInfo>is calculated and signed, then stored in the element <SignatureValue>.

Step 5. If the information of public key is required, it is stored in the element <KeyInfo>. This is a certificate of X.509 for sender and needed to confirm the digital signature. The procedure for confirmation is shown in Fig. 10.

Step 6. Finally, the XML digital signature is generated by including all created elements to the element <Signature>.

Fig. 8 shows the procedures to confirm the reliability of digital signature.

The information of certificates is extracted from the element <KeyInfo>to confirm the generated digital signature. It is compared to the certificate stored in the root certificate registry. Then the reliability is ensured.

In our works, we applied our model to mobile financial applications are likely to be one of the most important components of m-commerce as in figure 11. They could involve a variety of applications such as mobile banking and brokerage service, mobile money transfer, and mobile payments as shown in the figure 11. One interesting mobile financial application is micro payment involving small purchases such as vending and other items. A mobile device can communicate with a vending machine using a local wireless network to purchase desired items. Micropayments can be implemented in a variety of ways. One way is that the user could make a call to a certain number where per minute charges equal the cost of the vending item.

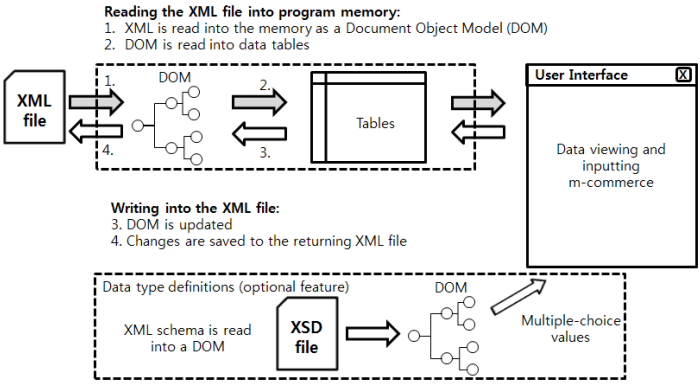

Fig. 10 Confirmation of Reliability of Mobile Security Model

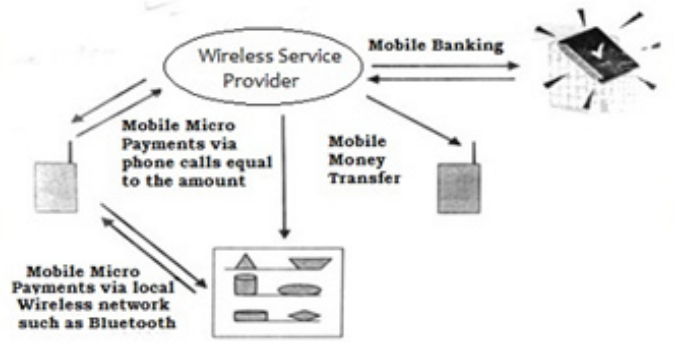

Fig. 11 One Execution example of M-commerce Services

4 Conclusion and Further Study

M-commerce introduced several new classes of applications, reviewed networking requirements, and discussed application development support. Since the area of mobile commerce is very new and still emerging, several interesting research problems are currently being addressed or should be addressed by the research and development community. It is believed that user trust will play a crucial role in acceptance and widespread deployment of mobile commerce applications.

Regarding m-payment, some systems are under development or already operational. One of the main future challenges will be to unify payment solutions, providing the highest possible level of security.

In this paper, PKI-based digital signature is designed based on XML and web services. It ensures the secure trading and non-repudiation in E-Commerce. The XML digital signature is designed and the operation structure is also proposed when two companies exchange the trading information as the form of XML messages. By using the concepts of proxy and web service, the conventional application programs can be operated without change. All information for document exchange is represented in XML. Only the secret information of XML document is encrypted. Because the digital signature is executed whole document, the security of trading and non-repudiation are guaranteed.

In the future, we will research for connecting to the CA, distribution of CRL (Certificate Revocation List) and key renewal for CA for improvement our model.

References

1. The Napster.com home page, `http://www.napster.com`
2. Chari, S., Kermani, P., Smith, S., Tassiulas, L.: Security Issues in M-Commerce: A Usage-Based Taxonomy. In: Liu, J., Ye, Y. (eds.) E-Commerce Agents. LNCS (LNAI), vol. 2033, pp. 264–282. Springer, Heidelberg (2001)

3. RFC: 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP (1996)
4. W3C, Extensible Markup Language (XML) (1998), http://www.w3c.org/XML
5. XML Signature Requirements WD, W3C Working Draft (October 1999), http://www.w3.org
6. Cho, K.M.: Framework of Content Distribution in Mobile Network Environment. In: Proc. the 2003 International Conference on Internet Computing (IC 2003), pp. 429–434 (2003)
7. http://www.roseindia.net/services/m-commerce/mobile-commerce.shtml
8. XML-Signature Syntax and Processing, W3C Recommendation (February 2002), http://www.w3c.org
9. XML Encryption Syntax and Processing, W3C Working Draft (October 2001), http://www.w3c.org
10. Decryption Transform for XML Signature, W3C Working Draft (October 2001), http://www.w3c.org
11. Takase, T., et al.: XML Digital Signature System Independent Existing Applications. In: Proc. the 2002 Symposium on Application and the Internet, pp. 150–157 (2002)
12. Xavier, E.: XML based Security for E-Commerce Applications. In: Eighth Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems, pp. 10–17 (2001)
13. Cho, K.M.: Packaging Strategies of Multimedia Content in DRM. In: Proc. the 2003 International Conference on Internet Computing (IC 2003), pp. 243–248 (2003)
14. Cho, K.M.: Web Services based XML Security Model for Secure Information Exchange in Electronic Commerce. The Journal of Korean Association of Computer Education 7(5), 93–99 (2004)