Development of A Common Payment Platform based on Interoperable Standards in Thailand

Somnuk Keretho
Institute for Innovative IT
Kasetsart University
Thailand
sk@ku.ac.th

Wisit Wongwilai
Institute for Innovative IT
Kasetsart University
Thailand
wisit@eng.ku.ac.th

Chutima Paiboonapibal
Institute for Innovative IT
Kasetsart University
Thailand
chutima@eng.ku.ac.th

Choak Visavayodhin
Master Science of Information Technology Program
Kasetsart University, Thailand
choak@debuz.com

Nansinee Sinjira
Master Science of Information Technology Program
Kasetsart University, Thailand
jinny_jny@hotmail.com

Abstract
In this paper, we describe an architecture framework and development approach of a national payment platform as a collaborative effort by the Bank of Thailand and representatives from Thai’s Banker Association, national research institutes and academy. We describe an XML/ebXML-based interoperable framework, and a proof of concept for developing an Interbank Transaction Management and Exchange system. We also give an overview of the related interoperable standards and our development tools.

Keywords: Payment systems, Interoperable standards, Common payment platform, XML, ebXML

1. Introduction
Thai payment systems have undergone over two decades of development and are now at a crossroads, responding to rapid market and technological changes, coupled with demands for high speed and security in making electronic commerce payments. Payment 2004, a road map for Thai Payments System was proposed in 2001 as a co-operative effort on part of the central bank and the market to review the current payment infrastructure and to chart a strategic map to lay down strong future foundations for the country’s payment systems [1]. This road map has been spearheaded by three lead institutions, the Bank of Thailand, Thai Bankers’ Association (TBA), and the National Electronics and Computer Technology Center (NECTEC). Payment 2004 identifies the key challenges, and proposes the necessary development directions. These challenges fall into five major areas. The payment infrastructure is one in five major areas. The key driver of this payment infrastructure is the need to develop a common payment platform based on interoperable standards to reduce duplicative payment infrastructure investments including inter-bank e-payment transaction over the Internet and to support the growth of e-commerce (Anat 2002).

This paper presents an approach to design the architecture framework and its relevant standards based on XML/ebXML specifications. This paper is organized as following. First, prior work on the Thailand’s existing payment systems is reviewed. Next, the architecture and framework of the Interbank Transaction Management and Exchange system (ITMX) are described. Then ITMX proof of concept development and the results are also discussed. Finally, the concluding remarks are presented.
2. Thailand’s existing Payment Systems

Presently, many Thai payment providers have accommodated the variety ways of the payment services to suit different needs, to provide different value-added services and to cope with demands for effective, convenient and secure transaction supporting electronic commerce payments. However, the current payment systems cannot interoperable among the different providers. In this section, we discuss the existing payment systems in Thailand and analyze a gap in these services.

2.1 Interbank payment systems

Payment systems in Thailand were supported by many payment providers. Each payment provider provides for payment transfer among its own member banks. There are many proprietary setups supporting specific payment needs as the following:

- ORFT
  Online Retail Fund Transfer (ORFT) provides the payment and fund transfer services among the members. The payment or fund transfer can be processed via the ATM (Automated Teller Machine) on the ATM pool network. ORFT has 13 banks registered as its members (Bank of Thailand 2003) in 2003.

- B2B e-Payment
  B2B e-Payment provides the payment and account transfer among its member via Internet. It focused on e-commerce payment transaction over the Internet. As of 2002, there are seven banks registered as its members.

- BAHTNET
  The Bank of Thailand Automated High-value Transfer Network (BAHTNET) is a large-value, on-line and real-time gross settlement (RTGS) system. BAHTNET provides finality and irrecoverable funds transfer across the accounts of member institutions held at the Bank of Thailand (BOT). BAHTNET is designed as an interbank funds transfer system for commercial banks and financial institutions with BOT accounts, as well as for third party credit transfers by the general public who can use the service to transfer funds nationwide (Bank of Thailand 2003).

- SMART
  The Bank of Thailand developed inter-bank retail funds transfer system called “Media Clearing” to eliminate the limitation of inter-bank funds transfer in the past that a payer and a payee had to open deposit accounts at the same bank. Media Clearing is designed as a batch system using electronic media such as magnetic tapes and diskettes. Later, the BOT enhanced the system to transfer data via on-line using web technology and changed the name from “Media Clearing” to “SMART” (System for Managing Automated Retail Funds Transfer). SMART now operates on both on-line and off-line basis to accommodate services with large volume, advanced agreement and regular payment interval. (Bank of Thailand 2003)

2.2 Intrabank payment systems

Payment transfer systems which link to many banks are summarized here:

- Trade Hub
  Trade Hub supports the payment transaction via Internet for e-commerce transaction. The merchant and the buyer have to open their accounts in the same bank. In 2002, Trade Hub has 6 banks registered as its members.

- Internet Banking
Internet Banking is a new service channel supported by several commercial banks. This system provides the payment and transferring service via Internet. Again, the payer and the payee have to open their accounts in the same bank. Fifteen banks provide these services in Thailand in 2002.

- **FEDI (Financial Electronic Data Interchange)**
  FEDI is the electronic payment system. The importer and the exporter can pay their import and export tax using the FEDI system. FEDI uses the UN/EDIFACT standard for data interchange between the traders to the Krung Thai Bank Pcl. and Thai Customs Department.

### 2.3 A need for common standards

Research results from the Bank of Thailand and the Thammasart University Research and Consulting Institution (TU-RAC) (Center for E-Commerce Infrastructure Development 2003) study suggested the following. Firstly, the market raised concerns on high systems development costs for a lack of standards and steep learning curves for consumers in switching standards.

Second, a majority of commercial banks supported the need to develop common standards for electronic bill presentment and payment, Internet banking, and mobile banking. A common payment platform would aim for a complete straight through processing (STP) of payments in the long-term (Anat 2002).

As described in the section of the Interbank payment systems, existing payment systems do not support on-line and real-time e-commerce funds transfer for Internet interbank transactions. The new payment systems should be designed to close the gap of interbank transaction for online and real-time e-commerce payment transaction through the Internet.

### 3. ITMX (Interbank Transaction Management and Exchange)

#### 3.1 Objectives

The purpose of the ITMX (Interbank Transaction Management and Exchange System) is to develop a common payment platform based on an appropriate interoperable standard to reduce duplicative payment infrastructure investments and to support the growth of e-commerce.

For a payment provider, ITMX is the central infrastructure and system for message and transaction exchange among the payment gateways and/or the commercial banks. ITMX also manages and processes the payment transactions among several banks. ITMX is the core infrastructure that provides the standard for interoperable with these following key features: 1) To be based on an open platform for cross platform connectivity. 2) To provide the message standard specification for interbank payment transactions. 3) To support the need to develop common standards for electronic bill presentment and payment, Internet banking and mobile banking as the online transaction processing. 4) To provide the secure and reliable system.

Figure 1 illustrates our proposed ITMX architecture framework. The framework picture shows the components of the ITMX system and the connection among ITMX, the payer bank and the payee bank. This figure also shows the components for the connectivity with the legacy system within the banks.
3.2 Interoperability Standard
The major objective of ITMX initiative is to harmonize payment standards, including the message types and the payment instruction. Our goal in this section is to discuss an interoperability standard that we are currently adopting as a basis for advancing the ITMX implementation.

3.2.1 Standard Messages
There are many message standards for finance and banking application. We focus on three messages as alternatives for our ITMX framework and proof of concept implementation.

IFX (Interactive Financial eXchange): The Interactive Financial eXchange (IFX) is a mature, well-designed XML-based, financial messaging protocol, built by financial industry and technology leaders incorporating decades of combined experience and best of breed design principles. (David et al. 2001) The goal for IFX has been two folds: 1) To use real business use cases and develop content that is meaningful and useful to the financial services industry. 2) To create a strong, flexible, open architecture that will support extending the protocol in an efficient, interoperable manner. IFX is built by several industry experts who have experiential defined, modeled and incorporated real-life use cases to produce relevant and useful business data objects.

SWIFT (Society for Worldwide Interbank Financial Telecommunication): SWIFT is the industry-owned cooperative supplying secure, standardized messaging services and interface software to the financial institutions around the world (ebXML Requirement Team 2001). SWIFT has announced the “SWIFT Standards XML.” This standard explains what the various XML components are, how they relate to the “SWIFT Standards Financial Dictionary”, and how the “SWIFT Standards Financial Dictionary” is organized to promote reusability (ebXML Requirement Team 2001).
**Online Retail Fund Transfer (ORFT):** ORFT system is the interbank online retail fund transfer service via ATM (Automatic Teller Machine) in Thailand. This system allows the customer to request money transfer transaction from its account in one bank to a third-party account in another bank. ORFT message is the message format defined for transferring in the ORFT system.

As discuss earlier, these three standard messages has different pro and con. For the ITMX proof of concept, we focused on the IFX standard message with these following reasons:

- Open standard: the open standard can exchange messages with international institutes in the future.
- Financial message: IFX is the standard message designed for financial message exchange that covers interbank fund transfer characteristics.
- Ease of Use: It is easy to use because the message is in XML format.

In the ITMX proof of concept, we recommend some message elements from IFX. Payment Add Request `<PmtAddRq>`, Payment Add Response `<PmtAddRs>`, Payment Reversal Request `<PmtRevRq>` and Payment Reversal Response `<PmtRevRs>` are the basic selected messages.

### 3.2.2 ebXML Message Service

The ebXML Message Service is the specification under the ebXML initiative. The ebXML (Electronic Business using eXtensible Markup Language), is a modular suite of specifications that enables enterprises of any size and in any geographical location to conduct business over the Internet. ebXML is an initiative of OASIS (the Organization for the Advancement of Structured Information Standards) and the UN/CEFACT (United Nations Centre for Trade Facilitation and Electronic Business). ebXML Message Services (ebMS), now endorsed as an ISO/DTS 15000-2 standard, is conducted within the OASIS technical process, because of the Consortium’s expertise in XML standards development (Electronic Commerce Promotion Council of Japan 2004).

The ebMS defines the message enveloping and header document schema used to transfer ebXML messages over a communications protocol such as HTTP or SMTP and the behavior of software sending and receiving ebXML messages. The ebMS is defined as a set of layered extensions to the base Simple Object Access Protocol [SOAP] and SOAP Messages with Attachments [SOAPAttach] specifications (IFX Forum 2003). The ebMS is also a closely coordinated definition for an ebXML message service handler (MSH). ebMS can be used to manage the ITMX as follows:

- The ebMS is recommended for implementation of securely sending and receiving any format of electronic documents. The prime objective of ebMS is to facilitate the exchange of electronic business messages within an XML framework. Business messages, identified as the ‘payloads’ of the ebXML messages, are not necessarily expressed in XML. XML-based messages, as well as traditional EDI formats, can be transported by the ebMS. The ebMS payload can take any digital form—XML, ASC X12, HL7, AIAG E5, database tables, binary image files, etc. (IFX Forum 2003)
- The ebMS is the high level protocol standard which is able to exchange the ebXML messages in many transportation protocols such as HTTP, HTTPS, SMTP, and FTP. Our proof of concept system uses HTTP and HTTPS for the transportation protocol. We used the HTTP protocol for the normal transaction and HTTPS protocol for the high security case.
- Reliable Messaging Module defined in the ebMS relates to delivery of ebXML messages over the communications channels. The ebMS defines the interoperable protocol such that two MSHs can reliably exchange with following features:
  - Persistent Storage and System Failure Handling
  - Message Acknowledgement and Message Retransmission Handling.
  - Duplicate Message Handling
- The ebMS provides the Security Module for handling the security risk as follows:
  - Encoding the data between exchanging with SSL version 3.0
  - Verifying the receiver (Sever Authentication) with Server Certificate
  - Verifying the sender (Client Authentication) with Client Certificate
  - Confirmation of sender’s document by using signature from ebXML Header and business document (Payload)
  - Confirmation of receiver’s document by using Acknowledgements which have electronic signature.

3.2.3 Collaboration Protocol Profile and Agreement
Collaboration Protocol Profile and Agreement (CPPA) is the specification adopted under the ebXML initiative, and now an ISO/DTS 15000-1. The Collaboration Protocol Profile (CPP) defines the capabilities of a Party to engage in electronic Business with other Parties. The Collaboration Protocol Agreement (CPA) defines the way two Parties will interact in performing the chosen Business Collaboration (IFX Forum 2003). Both Parties shall use identical copies of the CPA to configure their run-time systems to ensure that their systems are compatibly configured to exchange messages.

As described in the previous section, the ebMS can be used to define for an ebXML MSH. Typically, the software that performs the message exchanges and otherwise supports the interactions between the parties is middleware that can support any selected Business Collaboration. The ebXML MSH is used to exchange the message corresponded with the CPA.

3.3 The Example of Payment Scenarios
To understand requirements of the system thoroughly, ITMX initiative team has identified the business workflow in several cases to determine the features of the system and to study its feasibility in business and technical areas of development. Figure 2 illustrates the model of fund transferring in a case that the customer/payer and the merchant/payee have their accounts in the same bank. Therefore in the payment transaction in this case is not needed to transfer through ITMX.
Scenario B as in Figure 3 illustrates the payment transaction model in a case that the account owner’s bank is the payer bank. The payer bank registers payment instruction and requests for the payment with <PmtAddRq> (Payment Add Request) designated message to ITMX. The ITMX system will process the message and forward it to the designated payee bank.

Payment service C1.1 in Figure 4 illustrates the payment transaction model in case of an interbank fund transfer. The credit transaction was requested by the payee bank to the other payer bank through the ITMX system. ITMX will send verifying request and payment instruction to the payer bank. The payer bank will authenticate and verify the requested
information, and debit the payer’s account. This model could be utilized when no other Certification Authority (CA) is available.

Figure 4. Scenario C1.1: Account Owner Bank is the payee bank, the other bank is payer bank (In case of no Certification Authority-CA)

Payment services scenario C1.2 illustrated in Figure 5 is an interbank fund transfer case. A difference between scenario C1.1 and scenario C1.2 is that ITMX sends only the request to the payer bank for authentication at the first step. ITMX will send <PmtAddRq> message after receiving the confirmation of verification from the payer bank. This scenario is more maintainable and scalable.

Figure 5. Scenario C1.2: Account Owner Bank is the payee bank, the other bank is the payer bank (In case of no CA)

Figure 6 illustrates an exceptional flow (error handling) of the payment transaction. This case is similar to scenario C1.2, the difference is that the payee bank cannot credit the account after receiving the payment add request message <PmtAddRq>. The payee bank will send response message to ITMX with the payment reversal request <PmtRevRq>. The ITMX
system will forward the payment reversal request to the payer bank for reversing the payment transaction.

Figure 6. Scenario C1.3: Account Owner Bank is the Payee Bank, the other bank is the Payer Bank (an exceptional case of credit unsuccessfully)

4. ITMX Proof of Concept Development
The objective of the ITMX proof of concept development is for analyzing the feasibility of the common payment platform based on interoperable-based development.

4.1 Tools
As described in the section of Interoperability Standards, the ebXML Message Service Handler is the middleware for exchanging the message. We have developed the open-source software namely Lighthouse MSH to support this infrastructure. The Lighthouse MSH was developed by the Institute for Innovative IT, Kasetsart University and compliance with the ebXML Message Service Specification Version 2.0. Lighthouse MSH was developed by enhancing the open-source software named Hermes MSH (OASIS ebXML Collaboration Protocol Profile and Agreement TC 2002).

Figure 7 shows the Lighthouse MSH architecture. The Lighthouse client will send and receive the documents by connecting with the Lighthouse server. The Lighthouse server will create the ebXML message and send to the destination MSH by the configuration in CPA setting on the server. The Lighthouse server also extracts the payload from the received ebXML message and sends the payload to the Lighthouse client.
4.2 Test cases and results

To analyze the feasibility and impact on reliability and security, we focus on three major areas. We adopted some part of the ebXML Interoperability Test Specification (OASIS ebXML Messaging Services Technical Committee 2002) for our test cases. These test cases were used to ensure that the conceptual of the ITMX system is workable on both technical area and business area.

4.2.1 Reliable Messaging Test

ebXML Interoperability Test Specification categorized the test case to 5 terms as T1-T5. The reliable messaging test was identified in T5. We defined the two test cases in this interoperability test. Each test case indicates that the receiver can receive the message.

TR1-1: One way reliable messaging with XML payload: TR1-1

Sender sends a message with a small size payload (248 bytes) in XML format. Receiver receives the message and sends back an Acknowledgement message as shown in Figure 8.

TR1-1 requested the Lighthouse MSH to send a payload. The Lighthouse client will send the document by reading the payload in the outbox folder then sending to Lighthouse server. The Lighthouse server will create an ebXML message by the configuration in CPA. The receiving document will come in to the Lighthouse server, then the server will extract payload to the inbox folder which is defined in the client configuration as illustrated in Figure 9.
The result of TR1-1 testing, we have got the useful information for improving ITMX prototype as the following:
- The response time for sending/receiving a document via the Internet is not consistent although the document size is not changed. Speed of sending/receiving on Internet up to many environments are difficult to control because of Internet is an open environment.
- In case of sending documents through the Firewall, the result of receiving will take more response time.
- The Lighthouse MSH client (V.0.1b) was configured to the file system format. The concept of sending and receiving the message as the file system through the “inbox” and “outbox” folder is not suitable for the ITMX real time system.

**TR1-2: Two ways reliable messaging with XML payload: TR1-2**

As described in the previous test case, the TR1-2 test case was defined to improve the client program in order to the real time transmission. Lighthouse MSH client v.1.0b was developed for receiving message and direct sending to the backend system as shown in Figure 10 and Figure 11.
4.2.2 Business Work Flow Testing
From the business perspective, we test the business workflow as described in the section of the example of payment scenarios. We selected the following scenarios for the business work flow testing.
- Scenario C1.2: In case of Account Owner Bank is Payee Bank and other bank is Payer Bank (without CA).
  **The reason for choosing C1.2 situation**
  Scenario C1.2 is a situation that the business workflow involves many functions by relevant users (Payee Bank, Payer Bank, ITMX) so we will get useful results for developing an interbank fund transfer in case of a usual process.
- Scenario C1.3: In case of Account Owner Bank is Payee Bank and other bank is Payer Bank, this scenario represents an exceptional flow.
  **The reason for choosing C1.3 situation**
  Scenario C1.3 is an exceptional case. This test case is utilized to ensure that the system can manage an unsuccessful payment transaction.

4.2.3 Security Testing
Businesses have a high level requirement that appropriate security technology be applied to protect information involved in business processes. Aspects of security may be required at various layers of a business process; at an outsourcing/transaction layer, at a session layer (i.e., for the duration of a network session in which data is exchanged) or applied to a single, stand-alone document instance. In addition, application of security to a particular exchange or document instance must be determined by the business needs, and allow unrestricted and unsecured interchanges if the business process requires this. All, some, or no security features may be required in any particular exchange of business information. The following requirements are our general security definitions (Payment Systems Group 2004):
- Confidentiality - Only sender and receiver can interpret document contents
- Authentication of sender - Assurance of the sender's identity
- Authentication of receiver - Assurance of the receiver's identity
- Integrity - Assurance that the message contents have not been altered
- Non-repudiation of Origin - The sender cannot deny having sent the message
- Non-repudiation of Receipt - The receiver cannot deny having received the message
- Archiving - It must be possible to reconstruct the semantic intent of a document several years after the creation of the document.
This section is the study of security implementation for the ITMX system implementation. Our Lighthouse MSH was proved and certified in the security testing level from ebXML Asia Committee. Related to the ebXML requirement specification, we applied the security technology as following:

- **Network Security**
  By using open environment such as the Internet for transmission document possesses several kind of risks. Therefore, the Message Services Handler (MSH) must provide at least the HTTPS or Secure Socket Layer (SSL) protocol for encryption the document before the transmission. Virtual or exclusive private network connectivity among banks members and ITMX is recommended as the network infrastructure for more security environment.

- **Data security**
  According to the confidentiality of documents, the payload on over the ebXML message envelope could be encrypted before sending. As described in the section of standard message, our selected standard is in the XML format. The XML encryption technology worked by W3C XML encryption working group is recommended for encrypting/decrypting documents in the ITMX environment.

- **Authentication**
  The ebXML Message Service specification provides the part of security module. For this specification, a Signed Message is any message containing a Signature element. An ebXML message is be digitally signed to provide security countermeasures. (IFX Forum 2003)

5. **Implications**

The focus of this study was to develop a common payment platform based on interoperability standards. ITMX proof of concept development represented to the reliability of the data transmission using Lighthouse MSH and IFX messages standard which developed based on ebXML specification as the interoperable standard. The response time of data transmission depend on the network bandwidth.

Two important reasons for the success of developing the national electronic payment system were the following. First, the transaction management and exchange systems should identify the requirement of the system architecture, security and interoperable standards for the parties. Second, the business scenario and business model should be agreed by the bankers association or the business committee. The business committee should identify the business process, the type of banking transaction in the system, the daily settlement process and the model for management the transaction fee.

6. **Conclusion**

According to a road map for Thai Payment Systems, this paper focuses on the need to develop an electronic payment infrastructure based on interoperable payment standards. Our study shows the selected interoperability standard for implementation the electronic payment infrastructure. The study presents the existing payment systems and the need of the common platform. We also show the technical model and the gathering requirement of the infrastructure and interbank payment standard. Our study presents the architecture framework and the proof of concept system to decrease risk in developing real system in the future.

To respond to the business needs, our team has designed many payment scenarios for considering data feasibility for proof of concept and relevant business process. Our team has chosen IFX as message formats for payment because IFX is designed for financial exchange in XML formats that can be easily processed. For its technical protocol, we utilize *ebXML Message Services (ebMS)* and *Collaboration Protocol Agreement (CPA)* for securely and
reliably sending/receiving documents. The ebMS and the CPA are recommended within the ebXML framework developed by The United Nations Center for Trade Facilitation and Electronic Business (UN/CEFACT) and Organization for the Advancement of Structured Information Standards (OASIS), and now endorsed as ISO/IDS 15000-2 and ISO/IDS 15000-1 respectively. The ebMS open specification is an electronic document exchange protocol between organization that provides the reliability and security features. The CPA technology is a captured party agreement in electronic forms. This XML/ebXML protocol fulfills the requirements within Thailand’s Electronic Transaction Law (2001) on the issuers of authenticity, confidentiality and encrypted integrity. In this project, we have recorded the result of message exchange in the part of sending/receiving XML documents. We prepare the full message exchange formats in the future in usual cases and exceptional cases that can happen in real situation.

Our ITMX architecture framework is developed based on an open and interoperable standard that supports cross-platform and vendor-independent system integration and connectivity. This framework helps lower the cost of inter-organization integration, but still maintains the requirements of reliable and secured environment. Our architecture framework and proof of concept systems have assisted the Thailand Payment Systems Committee to define the directive of the ITMX system. The selected interoperable standards are workable for developing the common payment platform. We also realized more requirements for developing the Message Services Handler tools (MSH). This brings us to develop the new version of Lighthouse MSH which adds new features for configuration of different transmission types. It can send messages as file systems and also seamlessly integrate message transmission with the back-end system.

7. References


