



"HRD Program for Exchange of ICT Researchers and Engineers 2011"

(Final Report)

of

"The Pubic Key Infrastructure for Information
Security with the use of Multi-Agent Systems"

February , 2013



R
RITSUMEIKAN

Ritsumeikan University , Japan (Rits))

Yatanarpon Teleport Co.,Ltd, Myanmar (YTP)



Project Name	<i>Public Key Infrastructure for Information Security with the Use of Multi-Agent Systems</i>
Institution Involved in Project	<i>Yatanarpon Teleport Co.,Ltd, Myanmar (YTP)</i> <i>Ritsumeikan University, Japan (Rits)</i>
Project Members	<ul style="list-style-type: none"> • <i>Dr. Fumio Hattori, Vice Dean, Professor, Department of Information and Communication Science, Ritsumeikan University (Rits)</i> • <i>Dr. Kazuhiro Kuwabara, Professor, Department of Information and Communication Science, Rits</i> • <i>Nilar Aye, Department Head, Yatanarpon Teleport Co.,Ltd (YTP)</i> • <i>Hlaing Su Khin, Deputy Department Head, YTP</i> • <i>Toe Toe Win, Operation Engineer, YTP</i> • <i>Tay Zar Ko Ko, Network Engineer, YTP</i> • <i>Mo Mo Zin Than, Operation Engineer, YTP</i>
Report compiled by	<i>Nilar Aye, Yatanarpon Teleport, Myanmar</i>
Project Period	<i>March' 2012 ~ Feb' 2013</i>
Reporting period	<i>17 August' 2012 - February' 2013</i>
Objectives of the Project:	
<p>The main objective of this proposal is to implement a common framework for interoperability between CAs from cross PKI domain to build trust and secure for electronic transactions.</p> <p>The second objective is to encourage the recognition of digital signatures within ASEAN and use of secured applications which can save time, lower operational cost, strengthen regional cooperation and facilitate the business sector. Moreover, we would like to transfer technical knowhow from Japanese researchers who have experience in agents, semantic web technologies and security issues.</p>	

Section One: Summary

The project named "Public Key Infrastructure for Information Security with the Use of Multi-Agent Systems" was submitted to APT and it has been selected on 27th March' 2012. Two professors from Ritsumeikan University, Japan and five staff from Yatanarpon Teleport, Myanmar are participated in the project. All members are correspondence each other for implementation since it has been selected. Four phases of project milestone is set during the period of (11) months. According to project scheme, APT transferred (60%) of the allotted budget (US\$-32,667) to YTP account at UOB Singapore on (June 12, 2012).

To implement exchange plan schedule such as determine Multi-Agent communication method, design certificate database, construction of trust model and etc., researchers from Myanmar are required to visit Japan. So, three project members from YTP had visited to Ritsumeikan University, Japan for ten days from (11th July' 2012 to 21st July' 2012).

During the implementation phase 3, Professors from Ritsumeikan University visited Myanmar for (5) days from (12th Oct' ~ 16th Oct' 2012). Professors advised us the method of agent communication, message type and database design. Then, we jointly prepared a paper in order to publish at international conference.

At final implementation stage, the paper submitted to the 5th ASIAN Conference on Intelligent Information and Database Systems (ACIIDS) had been accepted on (29th Nov' 2012). In order to proceed the project, APT transferred second payment (US\$- 20,000) to YTP account at UOB Singapore on (13th Dec' 2012). According to the exchange plan schedule, three researchers from Myanmar had visited to Ritsumeikan University from (9th January- 19th January' 2013). The program had been tested with digital certificates and updated again for secure transaction while visiting. Moreover, updated the paper again for camera ready version to appear in volume 7802 of the Lecture Notes in Computer Science Series by Springer. At the moment, not only the presentation materials are being prepared for the ACIIDS 2013 conference but also the system is being updated for betterment of the application.

Section Two: Activities and Progress

27 Mar' 2012 : Project Acceptance

April'~ July 2012 : Interim Report had been submitted

Aug' ~ Nov' 2012 : System Prototyping

: Japanese Professors visited Myanmar for exchanging expert opinion

- Discussed on method of agent communication,
- Defined message type
- Design database structure (Annex – 1)

: Prepared a paper to be published as a Computer Science notes

Dec'2012~ Present : Correspondence and individual work

: System Prototyping

: Visiting Ritsumeikan University for system testing, updating

- Finalized paper and prepared for Camera Ready Version
(Annex -2)

: Presentation materials are being prepared

: Updates the system for betterment of the application.

Section Three: Outputs

- **Annex – 1** (Presentation file : Public Key Infrastructure for Information Security with the use of Multi-Agent System)
- **Annex _ 2** (Conference Paper to be published in Springer Proceedings: " Multi-Domain Public Key Infrastructure for Information Security with Use of a Multi-Agent System") at Kuala Lumpur, Malaysia, Mar 2013

Section Four: Expected Outcomes

1. At least one international recognized paper has to be published

Remark : Research Paper has been accepted for Publication at the 5th ASIAN Conference on Intelligent Information and Database Systems (ACIIDS)

2. Construct a sample model of online application using digital certificates

Remark: Sample prototype has been implemented

Section Five: Financial Statement (for Second Transfer)

Transferred Amount (13 th Dec' 2012)	-	20,000 US\$
Previous Balance at YTP (Aug' 2012)	-	<u>6,429 US\$</u>
Total Balance at YTP	-	26,429 US\$
Total Expense (Aug' 2012 ~ Feb' 2013) (Annex- 3)	-	<u>26,342 US\$</u>
Final Account Balance at YTP (26,429 – 26,342) US\$	-	87 US\$

Section Six: Next Step

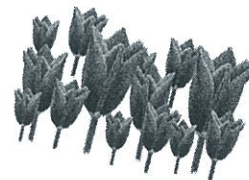
Feb' 2013 - Reporting

Duration of project	11 Months(Apr2012~Feb 2013)
Total Grant	54,445 US\$
Total Transferred Amount	52,667 US\$
Total Spent for the Project	52,580 US\$

Reporting Period	Final Report (Aug' 2012 ~ Feb ' 2013)			
Budget Headings	Total budget allocated/Estimated	Expenditure this reporting period	Total expenditure to date	Further information
Travel Expense (Airfare) Professors Trip to Myanmar	2,330 US\$	5,254 US\$	5,254 US\$	
Travel Expense (Daily Allowance and Accommodation Fees) Professors Trip to Myanmar	1,236 US\$	1,700 US\$	1,700 US\$	
Travel Expense (Airfare & Local Transportation) Myanmar Researchers Final Trip to Japan	4,242 US\$	4,500 US\$	4,500 US\$	
Travel Expense (Daily Allowance and Accommodation Fees) Final Trip to Japan	5,850 US\$	5,757 US\$	5,757 US\$	
Equipment Purchase Expenses	10,120 US\$	8,250 US\$	8,250 US\$	
Correspondence Expenses- Postal Charges	300 US\$	51 US\$	51 US\$	
Miscellaneous (Visa Fees, Conference Registration Fees)	4,995 US\$	830 US\$	830 US\$	
Total Expense until Feb' 2013			26,342 US\$	

Annex-1

" Public Key Infrastructure for Information Security with the use of Multi-Agent System"



**Presented By : Yatanarpon CA ,
Yatanarpon Teleport Co., Ltd.
Date : 15-October-2012**

CONTENTS

- Overview of the system
- Motivating Scenario
- Agent Implementation & Agent Communication
- System Architecture
- Trust Model Implementation & Database Design
- Conclusion

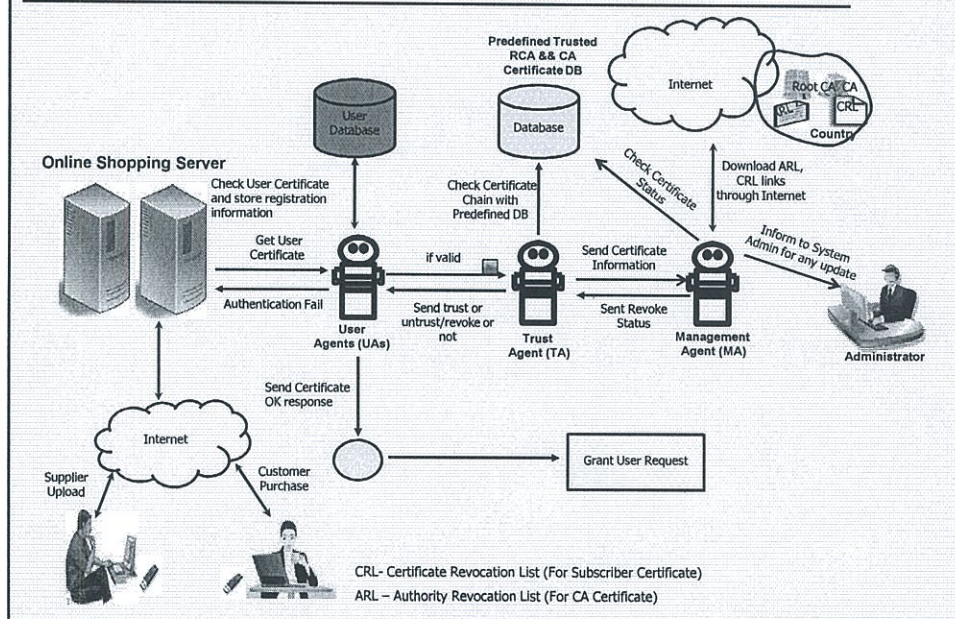
OVERVIEW OF THE SYSTEM

- Implement a system that increases the use of secure online applications **such as e-Government, e-Commerce, etc.**
- Use Public Key Infrastructure (PKI) for the authentication and authorization of the user
- Apply Multi-Agent technology to control access and manipulate the autonomous processes
- Use Java Language to implement the system.

OBJECTIVES

- To create a common framework for interoperability among CAs from multi PKI (Public Key Infrastructure) domains to build trust and secure for electronic transactions
- To encourage the recognition of digital signatures and use of secured applications in e-commerce area which can save time, lower operational cost and strengthen regional cooperation.
- To transfer technical knowhow from Japanese researchers
- To promote the development of advanced ICT for researchers in the Asia-Pacific region.

MOTIVATING SCENARIO



MULTI AGENT PROTOTYPING

Performing the issue of PKI interoperability supporting E-commerce.



User Agents (UAs)

- Validating client certificates such as certificate's public key, validity, key usage and enhance key usage.
- Storing user certificate information in the database.
- Negotiating each other for certificate usage and communicate with other agents in the system.



Trust Agent (TA)

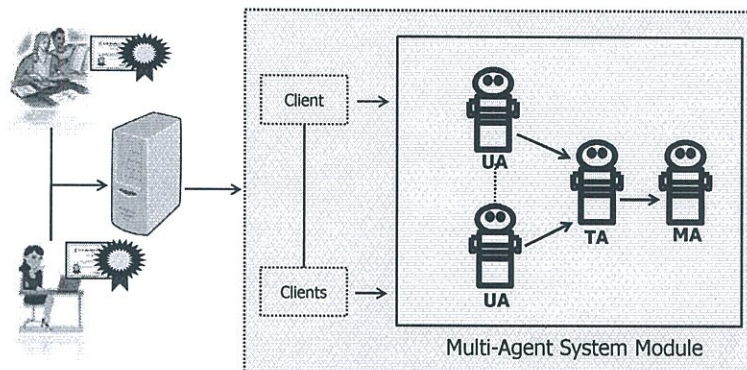
- Checking issuer certificate and its chain against with predefined Trusted Certificate Database.
- Sending message to Management Agent for additional checking.



Management Agent (MA)

- Keeping track of Trusted Certificate Database
- Verifying the status and validity of the certificate and informs to the administrator by messaging.
- Downloading ARL/CRL (Authority/ Certificate Revocation List) for checking of certificates whether any of them are included in the revocation list or not.
- Sending status message to UA for granting access and perform transactions securely.

AGENT CREATION

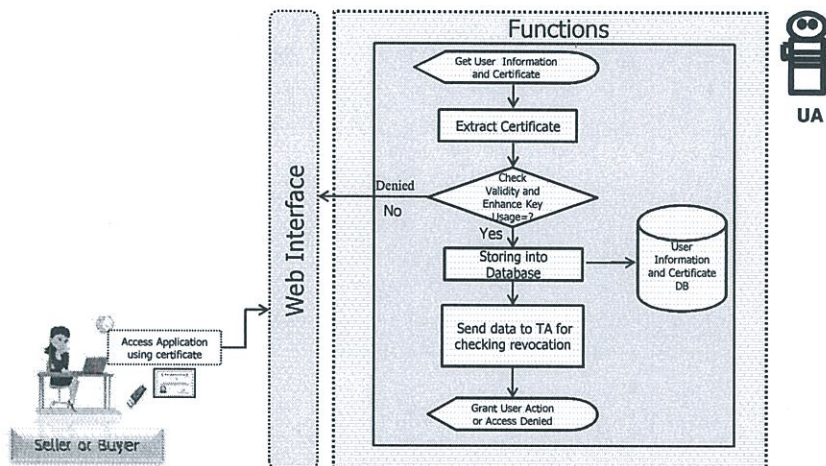


FUNCTIONS OF USER AGENT

Functions included :

1. Checking validity of user certificate
2. Extract various fields of certificate detailed information
3. Store certificate information into user database.
4. Send certificate information to Trust Agent to check trusted chain of the user certificate.
5. Manage messages from other agents
6. Negotiate for the same PKI domain certificates.
7. Accept or reject user actions and store user activity in the user activity log.

FLOW CONTROL OF USER AGENT

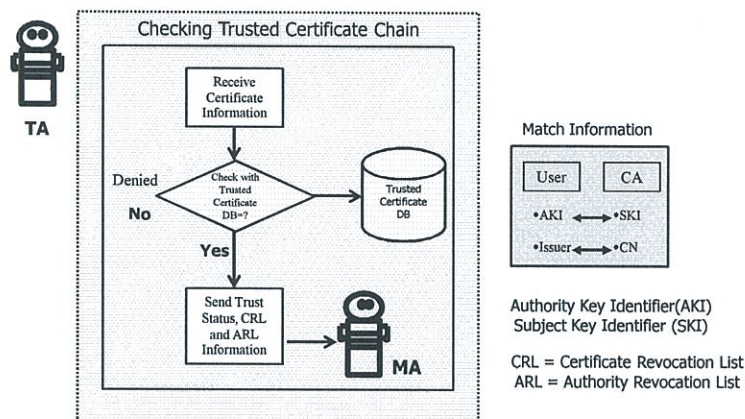


FUNCTION OF TRUST AGENT

▪Functions included :

1. Receive request from UAs
2. Check certificate information with DB
3. Reply message to UA, if certificate chain is not trust
4. Send certificate information to MA for revocation checking
5. Reply message to UA whether user certificate has been revoke or not

FLOW CONTROL OF TRUST AGENT

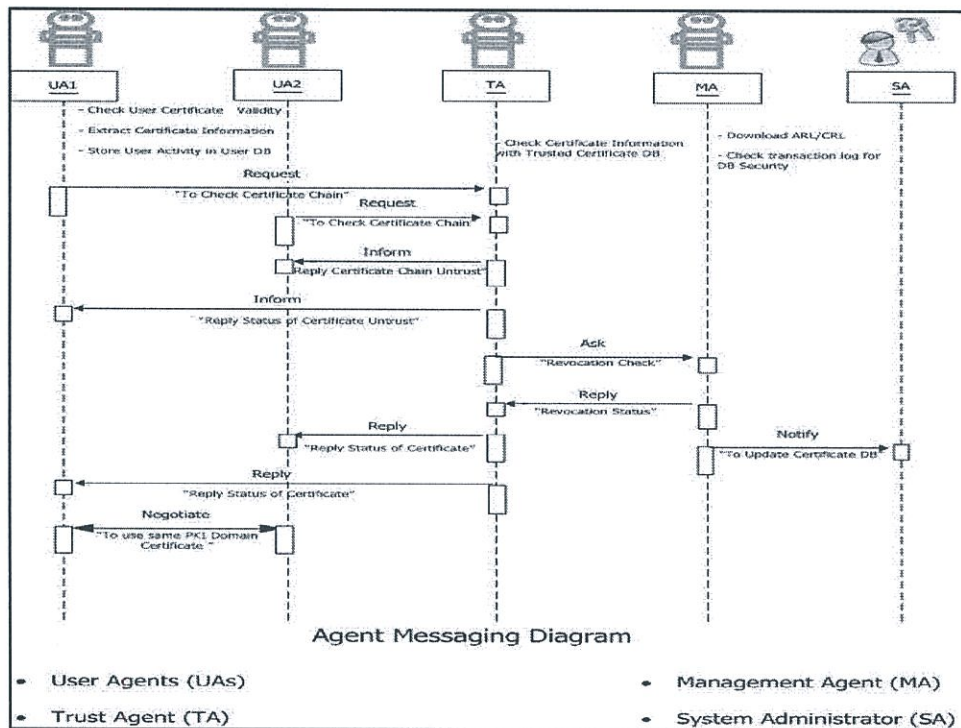
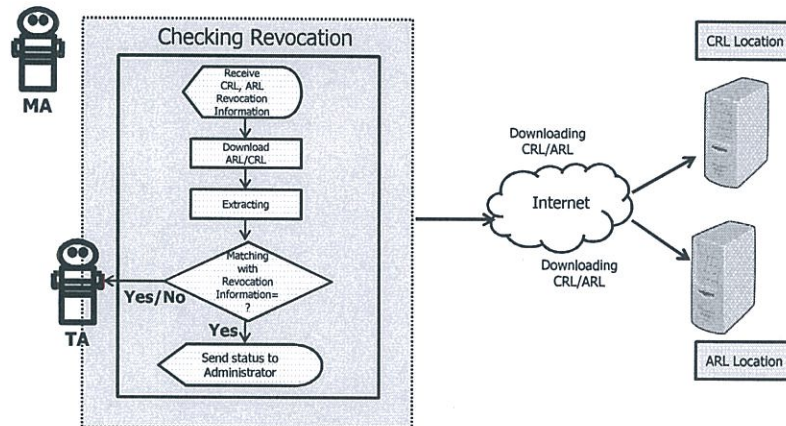


FUNCTION OF MANAGEMENT AGENT

•Functions included :

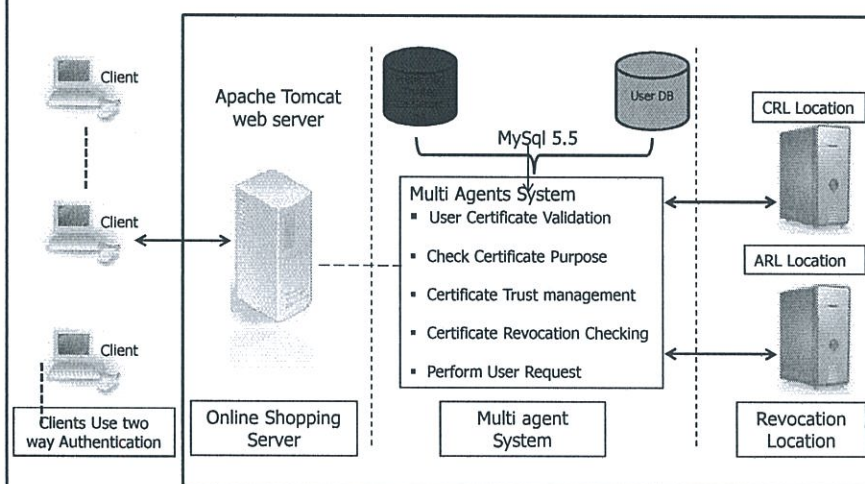
1. Receive message from TA
2. Download ARL/CRL from respective link
3. Reply revocation status to TA
4. Inform administrator for DB update, if any certificate has been revoke in predefined DB.
5. MA checks DB record for security and informs system administrator for any changes such as update, delete, insert.

FLOW CONTROL OF MANAGEMENT AGENT

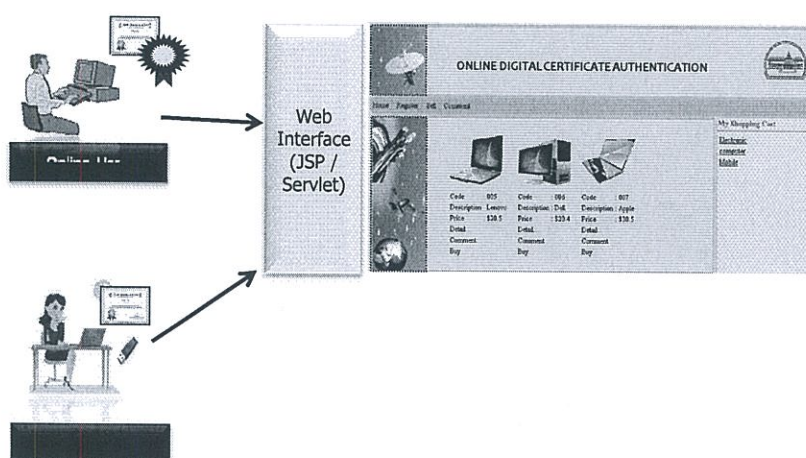


AGENT COMMUNICATION & IMPLEMENTATION

SYSTEM DESIGN



USER INTERFACE



SYSTEM DETAIL : WEB SERVER

- Server type : Dell (R720 Power Edge)
- Operating System : MS Window Server 2008
- Web server : Apache Tomcat
- Version : 7.0.29

DATABASE SERVER

- Server type : Dell (T310 Power Edge)
- Operating System : MS Window Server 2008
- Web server : My SQL
- Version : 5.5
- Databases
 - User Database, Trusted predefined Certificate Database.

SYSTEM DETAIL : CERTIFICATE SERVER

Root Certification Authority Server (ARL Provider)

- Server type : Clone
- Operating System : MS Window Server 2008
- Roles Service
 - Active directory Domain Service, Active Directory Certificate Service, Web Service.
- Function
 - Domain controller for network
 - Issues CA certificates
 - provide revocation information for CA

SYSTEM DETAIL : CERTIFICATE SERVER

Certification Authority Server (CRL Provider)

- Server type : Clone
- Operating System : MS Window Server 2008
- Roles Service
 - Active Directory Certificate Service, Web Service.
- Function
 - Issues end entity (user) certificates
 - Online web enrollment for Certificates
 - Provide revocation information for user certificates

TRUST MODEL IMPLEMENTATION

HIERARCHICAL TRUST MODEL

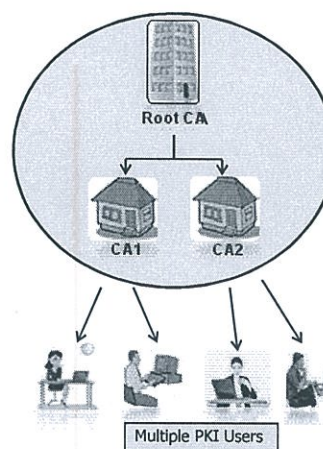
Root Certification Authority (Root CA)

- Root CA issues signing certificate to CAs.
- Root CA provides validation and revocation information (ARL) of CA certificates.

Certification Authorities (CAs)

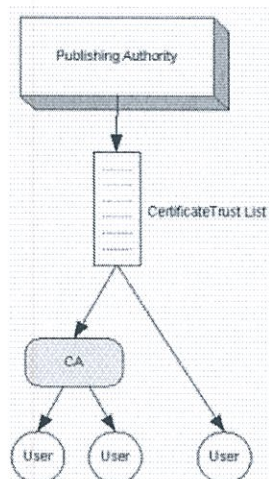
- CAs issue user certificate (end entity) certificate to users..
- CA provides validity and revocation information of (CRL) of user certificates

Single PKI Domain

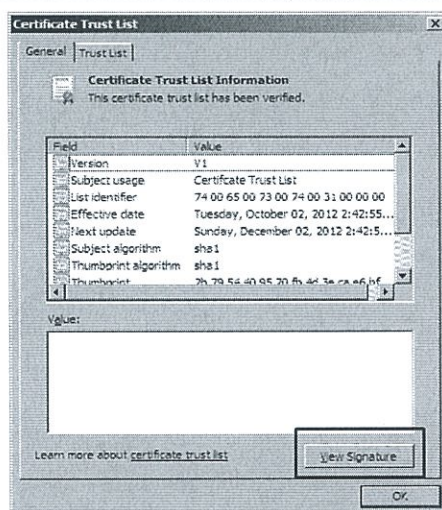


TRUST LIST MODEL

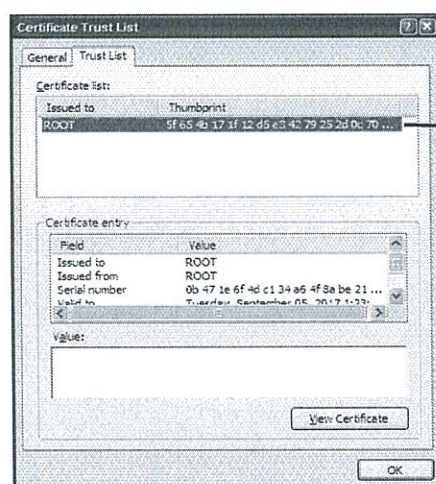
- Trust list model provide trust for third party self signed Root Certification Authority in enterprise domain.
- Trust list contains a collection of Root Certificate .
- It has been signed and verified by Trust List Signing Authority.



SAMPLE CERTIFICATE TRUST LIST

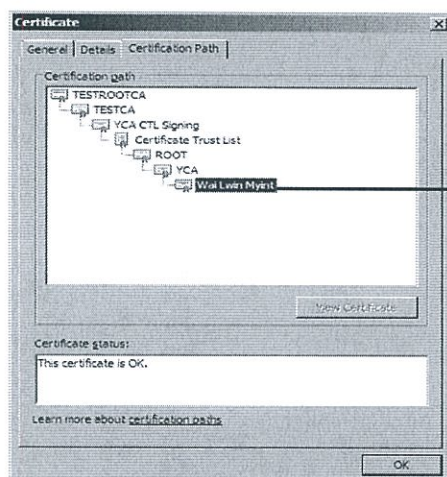


TRUST LIST : TRUST LIST PANE



→ List of root certificates contained in the trust list.

TRUST LIST CONT:



A sample client certificate trusted through Certificate Trust List.

DESIGNING DATABASE



User Activity Database



Predefined Trusted Root CA and CA Database

USER DATABASE

User's Certificate Table

userdb.usercertificate
UsercertificateId : int(10)
SerialNumber : varchar(100)
Issuer : varchar(100)
NotBefore : date
NotAfter : date
SubjectDN : varchar(100)
Email : varchar(50)
CommonName : varchar(100)
PublicKey : varchar(500)
CertificateType : varchar(50)
EnhancedKeyUsage : varchar(100)
SubjectKeyIdentifier : varchar(100)
AuthorityKeyIdentifier : varchar(100)
CrlDistributionPoint : varchar(100)
AuthorityInformationAccess : varchar(100)
Thumbprint : varchar(100)

Crl Distribution Point: Certificate Revocation List
Distribution Point

Seller Table

userdb.seller
sellerId : int(200)
username : varchar(100)
loginName : varchar(100)
email : varchar(100)
password : varchar(100)
accountNo : varchar(500)
accountInfo : varchar(600)

Buyer Table

userdb.buyer
buyerId : int(255)
userName : varchar(500)
loginName : varchar(400)
password : varchar(400)
email : varchar(500)
creditcardNo : varchar(600)
creditcardInfo : varchar(700)
accountInfo : varchar(700)

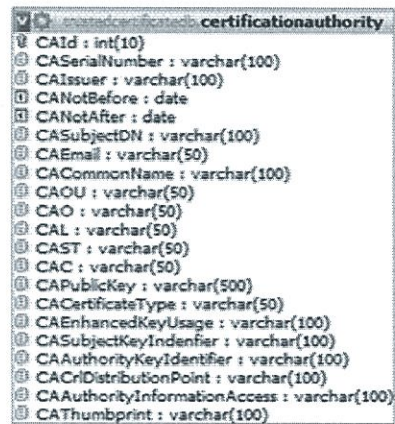
TRUSTED CERTIFICATE DATABASE

Certification Authority Table

trustedcertifiedb.certificationauthority
CAId : int(10)
CASerialNumber : varchar(100)
CAIssuer : varchar(100)
CANotBefore : date
CANotAfter : date
CASubjectDN : varchar(100)
CAEmail : varchar(50)
CACCommonName : varchar(100)
CAOU : varchar(50)
CAO : varchar(50)
CAL : varchar(50)
CAST : varchar(50)
CAC : varchar(50)
CAPublicKey : varchar(500)
CACertificateType : varchar(50)
CAEnhancedKeyUsage : varchar(100)
CASubjectKeyIdentifier : varchar(100)
CAAuthorityKeyIdentifier : varchar(100)
CACrlDistributionPoint : varchar(100)
CAAuthorityInformationAccess : varchar(100)
CAThumbprint : varchar(100)

TRUSTED CERTIFICATE DATABASE

Certification Authority Table



```

trustedcertificatedb.certificationauthority
CAId : int(10)
CASerialNumber : varchar(100)
CAIssuer : varchar(100)
CANotBefore : date
CANotAfter : date
CASubjectDN : varchar(100)
CAEmail : varchar(50)
CACommonName : varchar(100)
CAOU : varchar(50)
CAO : varchar(50)
CAL : varchar(50)
CAST : varchar(50)
CAC : varchar(50)
CAPublicKey : varchar(500)
CACertificateType : varchar(50)
CAEnhancedKeyUsage : varchar(100)
CASubjectKeyIdentifier : varchar(100)
CAAuthorityKeyIdentifier : varchar(100)
CACrDistributionPoint : varchar(100)
CAAuthorityInformationAccess : varchar(100)
CAThumbprint : varchar(100)
  
```

MILE STONE OF THE PROJECT

Phase 1 (Mar' 2012 ~ April' 2012)

- Define the work scope
- Determine Multi-Agent communication method
- Design certificate database

Phase 2 (May' 2012 ~ July' 2012)

- Construction of trust model
- System Prototyping
- Analyze methodologies

Phase 3 (Aug' 2012 ~ Nov' 2012)

- System Prototyping, Documentation

Phase 4 (Nov' 2012 ~ End of Jan' 2013)

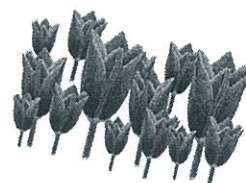
- System Integration, Testing, updating, Reporting

CONCLUSION

- The system is intended to provide the CA-CA Interoperability for multi PKI domains to build trust and confidence for e-transactions.
- A common framework has been proposed encouraging recognition of digital signatures within different regions.
- A useful and trusted security model for online applications and e-government applications.
- To apply the multi-agent system to control the strong authentication and flexible use of various applications by many clients.
- The system is mainly intended to support e-commerce



Thank you !!!



Annex-2

Multi-domain Public Key Infrastructure for Information Security with Use of a Multi-Agent System

Nilar Aye¹, Hlaing Su Khin¹, Toe Toe Win¹, Tayzar KoKo¹, MoMo Zin Than¹,
Fumio Hattori², and Kazuhiro Kuwabara²

¹ Yatanarpon Teleport Co., Ltd, Universities' Hlaing Campus, Yangon, Myanmar
{nilaraye, hlaingsukhin, toetoewin, tayzarkoko,
momozinthan}@teleport.net.mm

² College of Information Science and Engineering, Ritsumeikan University
1-1-1 Noji Higashi, Kusatsu, Shiga-ken 525-8577 Japan
{fhattori, kuwabara}@is.ritsume.ac.jp

Abstract. We propose a multi-agent based common framework for interoperability among CAs (Certificate Authorities) from multiple PKI (Public Key Infrastructure) domains to build trust and secure for electronic transactions. Most of the countries recognize PKI as a powerful technique for security services and implemented their own PKI for online user. Several trust models have been used in PKI, and achieving interoperability between them is a major issue which requires recognition of certificates from different domains in order to perform transactions confidently in a cross border application. In our system, User Agent, Trust Agent and Management Agent are created. These software agents co-operate each other for user authentication and authorization processes autonomously in multiple PKI domains within the ASEAN region to encourage the recognition of digital signature to enhance regional market. Our system intended to facilitate not only for matured e-commerce but also for individual start up entrepreneur for secure trading by taking into consideration of regional needs.

Keywords: Public Key Infrastructure (PKI), Multi-Agent System (MAS), PKI interoperability, Certification Authority (CA), Digital Certificate.

1 Introduction

Nowadays, the development of online services such as e-Government, e-Commerce, e-Procurement are growing tremendously whilst online fraud and misuse of personal information are also increasing by means of various attacks. Although the web site is being configured with user registration and authentication, user can give wrong information in the registration process. Therefore, verification of buyer and seller is required in an e-commerce arena in order to build trust. The technology of Public Key Infrastructure (PKI) [1][2] has been established to solve these issues such as data integrity, confidentiality, user authenticity, and non-repudiation of online users. With the use of digital certificates a user can identify who is a real buyer or seller as well as

individual or organization. However, users need checking manually the certificate's validity, whether it has been issued by trusted authority or not, and its status. According to the user's knowledge, this task would be troublesome as certificate checking processes are tedious and complicated. The situation may get worse when the buyer and seller are using digital certificates from different PKI domains. Therefore, we propose a system using PKI and multi-agent technologies to identify a user and authenticate user access to the system to support secured e-commerce. In this approach, software agents autonomously perform checking of the digital certificates' validity, certificate chain and certificate revocation status instead of a user. The major contributions of the system are:

- Strong authentication mechanism based on PKI ;
- Multi-agent cooperation for authentication of user access and validation of digital certificates from various PKI domains; and
- Implement a common framework for CA-CA Interoperability.

This paper is structured as follows. The next section describes the current issues regarding PKI interoperability, and Section 3 discusses some related works that apply the multi-agent concept to PKI. Section 4 presents the motivating scenario for the propose system. Section 5 describes the implementation of the proposed system. Section 6 discusses the merits of the proposed system, and the final section concludes this paper.

2 Current Issues in PKI Interoperability

Nowadays PKI is an important part of information security infrastructure. PKI based e-business security system [3] has been proposed as an effective solution for online commerce. There are different types of digital certificates issued from various CAs which represents an identity of online user. It can be used for a trust relationship and encrypt/decrypt user information for privacy and security. Most countries recognize PKI as a powerful technique for security services and implement their own PKI model for online users. Several trust models have been used in PKI. Analysis and comparison of PKI-based trust model are proposed in [4] to provide information security services. Although the use of certificate has been mutually recognized by each other within a region, achieving PKI interoperability [5] is required for cross border applications to facilitate business trust. Thus, interoperability among different PKI domains becomes an issue in order to promote cross border activities in electronic commerce.

A number of alternatives have been suggested for the PKI interoperability such as Cross-certification, Bridge CA, Certificate Trust Lists, Accreditation Certificate, Strict hierarchy and etc., in [6]. Besides, one of the proposals was presented for achieving inter-domain interoperability [7] and provided recommendations for the way forward. The CA-CA interoperability has been implemented in the European Union following the Trust List model. Although it has been initiated within ASEAN lately, granting mutual recognition will take time due to various constraints such as

legal issues, technical standards and so on. Therefore, a method is needed to verify digital certificates in a common application to build trust between users and to secure their information.

Another concern that needs to be taken into consideration is a process of certificate verification and validation by user him/herself who requires knowledge of digital certificate and online security. For instance, user certificate must not be expired, it has not been revoked including its signing certificate, and purpose of key usage must be standard for online applications. There are several steps require for a certificate validation. In order to be a legitimate certificate, for example, a buyer needs checking of a seller's certificate and its issuers' validity period. Besides, issuing authorities must be an authorized trusted third party. Afterwards, the buyer verifies all certificates' revocation status by using online services such as OCSP, LDAP or downloads ARL/CRL manually. These checking processes are complicated requiring autonomous actions which carry out one after another. Therefore, we propose a method to accomplish these issues with the use of a multi-agent system.

3 Related Works

There are a number of research works have been done on combination of PKI and multi-agent technologies. For example, the 'secret agent' concept was proposed, and KQML [8] was extended to handle public key management in [9]. The focus of this paper is on the development of an agent system itself which used KQML as an agent communication language and to make the agent system more secure. So, they introduced PKI into the agent system. In doing so, KQML was extended to include several new performatives to handle digital certificates. Their proposed 'secret agent' handles flexible configuration of digital certificate management. This approach does not pre-specify any particular certification format and hierarchical relationship in the software and it is dynamically formed as the agents apply/issue their certificates according to the desires of the applications. But, our proposed system uses pre-defined trusted database which stores certificates and its related hierarchies for verification by the software agent.

Another approach was introduced an agent-oriented public key infrastructure (APKI) for multi-agent e-service [10]. Its application to the digital certificate management was described in [11] by same authors. They argued that their proposed APKI provides a binding mechanism between human and agent so that the legal responsibility of agent can be traced to the corresponding human user. The proposed APKI was built on the FIPA-OS. In this approach, human and agent required certificates for identification which were explicitly separated in order to differentiate between human and agent certificates. Similar to our system, the activities such as authentication, authorization, access control, and trusted relationships are carried out by the use of PKI and multi-agent technologies. However, our proposal requires only user certificate which is used by an agent to identify user and control access of the system after certificate verification.

One more interesting approach also described the concept of multi-agent which is applied to the authentication in the multi-application environment [12]. By introducing an application agent (AA) corresponding to a particular application, the proposed system can flexibly handle the requirements of multiple applications. However, it does not consider the multiple PKI domains. The same authors propose in [13] similar to our system creating several agents for client certificate validation, authorization check, access granting and administration application delegation scheduling. Moreover, it employs PKI to build trust among agents. It is, however, different from our approach in that MAS subscribe to the CA and own the key pair and the certificate that messages among agents can be signed/verified and encrypted/decrypted with the basic PKI scheme. These agents look up the LDAP and verify the authenticity of the client certificate.

4 Motivating Scenario

E-commerce security is a serious issue [14] requiring strong authentication as well as authorization. A solution is needed to control an access of application of both buyer and seller which allows buying and selling can be done at the same place. Products posted on the site can be viewed by everyone. But, user registration is required for a new user and digital certificate is always necessary for whoever wants to engage in an activity such as buying, selling or giving comments to a product. The user can get digital certificate from any trusted third party or Certification Authority (CA) by paying certain fees which must be stored in an e-token, smart card or secured device. Together with a user certificate, its signing certificates and related chain are also included in it. Most of the digital certificates have been issued with one year validity. A system administrator keeps a user database and certificate database up to date and makes it secure by executing necessary steps.

In the motivating scenario, users can perform as a role of buyer or seller who does actions such as uploading product to sell, updating product information, buying something or giving comments. The buyer can identify the product owner easily since a digital certificate has been posted together with the product. When a user clicks to buy, the system automatically carries out verification and required negotiation processes to complete the transaction successfully. Then, a seller receives a notification email from the system and proceeds to the bank for payment confirmation. The user does not need to consider steps of certificates checking. The buyer, seller and bank cooperate with each other to achieve the business processes.

5 Use of Multi Agents

To implement a system that can execute the motivating scenario described above, we apply multi-agent technology. Multi Agent System (MAS) [15] is a technique where several agents communicate each other to solve problems that are difficult or impossible for an individual agent. In our system, User Agent(UA), Trust Agent (TA) and Management Agent(MA) are created which co-operate each other for user authentication and authorization processes (Figure 1).

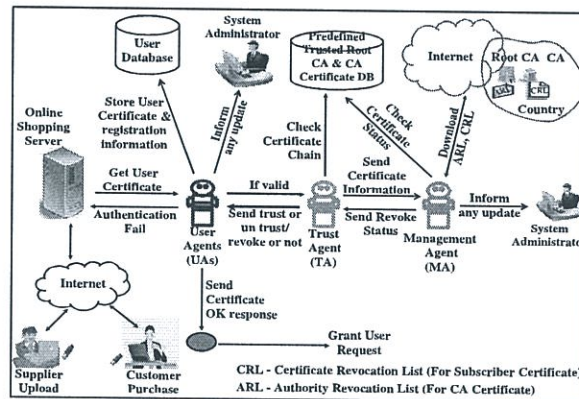


Fig. 1. Motivating Scenario as Implemented as a Multi-Agent System

User Agents are created for every user which is responsible for user authentication to validate the user certificate such as the certificate's public key, its validity and key usage. If the certificate is not valid, it rejects the user to enter the system. Prior to the expiration date, UA sends a message to System Administrator to inform the seller whose certificate will expire soon. If the user fails to update the certificate on time, the UA sends as notification to System Administrator to remove the product from the database. It also sends a message to the TA for revocation checking. The process flow of User Agent is shown in Figure 2.

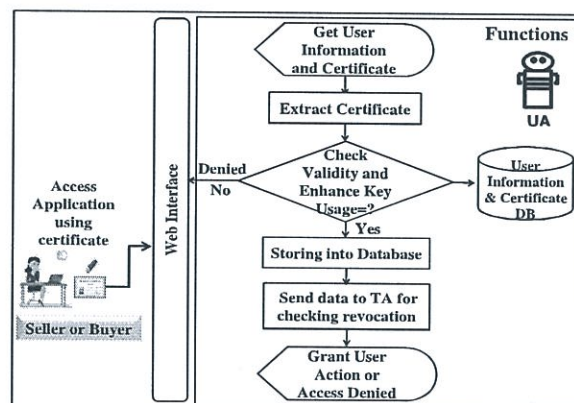


Fig. 2. Processes of User Agents

After receiving a message from UA, TA verifies the issuer certificate and its chain based on its trust model in the certificate Database. Suppose that the user certificate is issued from the Hierarchical model. If so, the authority key identifier (AKI) of the user certificate and the subject key identifier (SKI) of its issuer certificate (CA) must match, and AKI of CA certificate and SKI of its issuer certificate (Root CA) are

required to check by TA again. After these steps, TA sends a reply message to UA to decline user access or MA to examine the revocation status. The process flow of Trust Agent is shown in Figure 3.

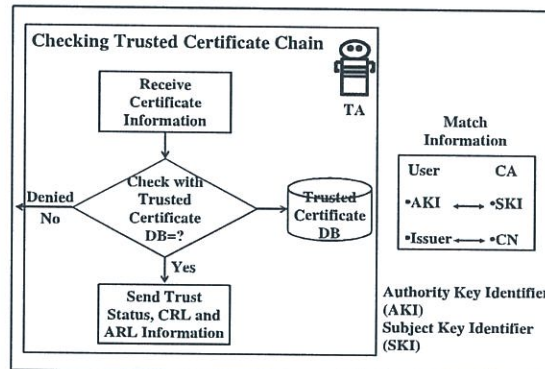


Fig. 3. The Processes of Trust Agent

MA receives the user certificate information from TA and retrieves Authority/ Certificate Revocation List (ARL/CRL) location from the database. MA downloads a file for checking of certificates. If any of them are included in the revocation list, MA replies to TA not to allow this user to the system. If not, it grants user to perform transaction securely. MA also keeps track of the Trusted Certificate Database for security whether it has been updated or amended. Besides, MA checks validity of certificates frequently and informs status to the administrator by messaging. The process flow of Management Agent is shown in Figure 4.

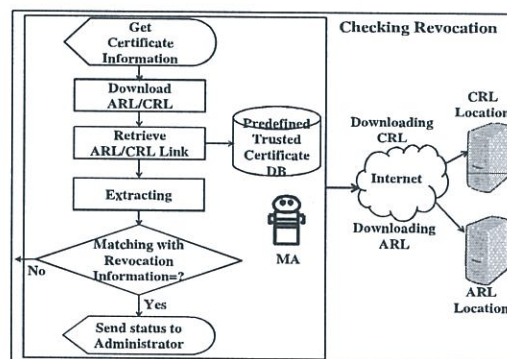


Fig. 4. The Processes of Management Agent

5.1 Messages in Agent Communication

In our proposed approach, we use Agent Communication Language (ACL) to communicate among agents by means of message exchange [16]. The popular ACLs are

Foundation for Intelligent Physical Agents (FIPA) [17] and Knowledge Query and Manipulating Language (KQML). In FIPA, several interaction protocols are defined and we follow its standard and specification for agent implementation. An example agent message exchange is described in Figure 5. In this example, UA extracts certificate into detail and checks validity and related information.

An access of user is denied, if certificate validation process fails. Otherwise, UA sends a "REQUEST" to TA to check the chain of user certificate. The latter checks the related certificate chain with the help of predefined trusted certificate database. For instance, a chain is a series of issuing authority certificates i.e., Root CA and CAs, etc. TA "INFORM"s an error message to UAs, if certificates are not matched with stored certificates which means it is not trusted. If not, TA "ASK"s MA for checking of the revocation status. Then, MA downloads the CRL file from the Internet and checks whether the user certificate or any of the issuing certificates are included in it. MA sends a "REPLY" message with a status of "Revoked or not" to TA. Afterward, TA sends a "REPLY" message to inform UA whether the user access to the system is granted or denied.

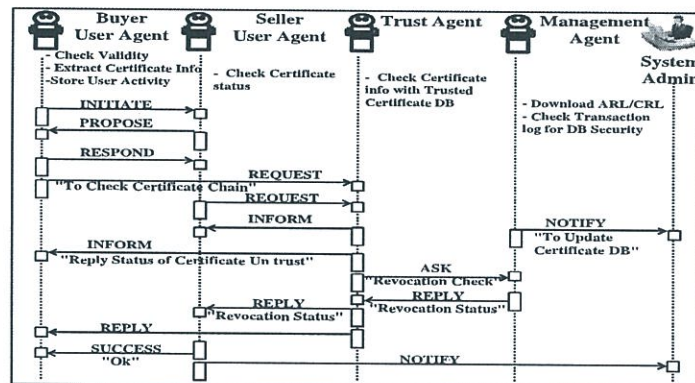


Fig. 5. Agent Communication Steps

The negotiation between user agents to decide on the PKI domain to use can be described as follows (Figure 6):

- UA (Buyer Agent) "INITIATES" with its own certificate to another agent (Seller Agent). If the user certificates are under the same PKI, the negotiation becomes successful and carries out the transaction.
- If not, the Seller Agent "PROPOSE" to Buyer Agent to provide a similar domain certificate
- Buyer Agent "RESPOND" the same PKI certificate to the Seller Agent
- Seller Agent sends "SUCCESS" message to complete the transaction

Message Type	Sender and Receiver of the Message	Meaning of the Message
Initiate	Buyer User Agent to Seller User Agent	To start transaction
Propose	Seller User Agent to Buyer User Agent	To propose for same PKI domain certificate
Respond	Buyer User Agent to Seller User Agent	To reply certificate is same PKI domain or not
Request	User Agents to Trust Agent	To check chain of user certificate such as Root CA and CA certificates
Inform	Trust Agent to User Agents	To respond the status of user certificate which is not trust
Ask	Trust Agent to Management Agent	To request the status of certificate revocation
Reply	Management Agent to Trust Agent Trust Agent to User Agent	To reply certificate revocation status, certificates have been revoked or not
Success	Seller User Agent to Buyer User Agent	To complete transaction

Fig. 6. Summary of the Agents Message

5.2 System Implementation

Java technology is applied to implement the system. We use Apache Tomcat for web service and MySQL for user database and trusted certificate database (Figure 7). They keep user, product, and certificate information. Software agents are created to control user access and activity of the system. Agent automatically downloads ARL/CRL files everywhere from the Internet.

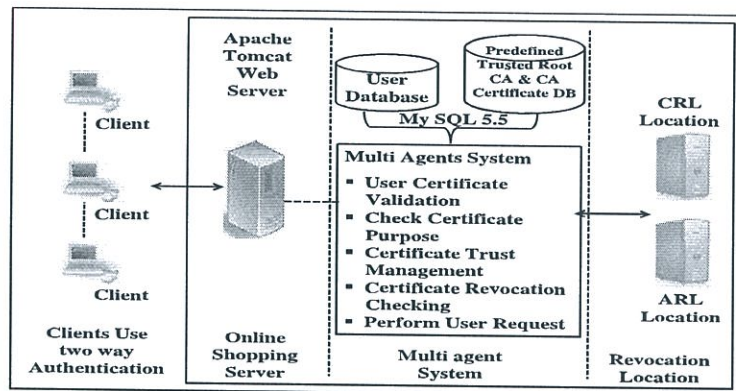


Fig. 7. Overview of the system

6 Discussion

Nowadays, the use of PKI becomes complex due to multi-domain and multi-vendor PKI with various implementations. The merit of our system is to ensure the multi-domains PKI interoperability [18] and to contribute the development and spread of reliable PKI in applications of future electronic society. The system will recognize different digital certificates by validating the certificate path and maintain trust entity. The proposed system has the following benefits.

- **User-Oriented-** The system is easy to be used by everyone from anywhere at any time. Also, it is not only user friendly but also simple from the user point of view which does not require additional hardware and software. Users can get digital certificate within their region with reasonable price.
- **Interactivity-** PKI based multi-agent system establishes user trust and secure channel within local and international organizations. It can operate in distributed, dynamic and open user environments which make it possible to enrich interactions of the system. The issue of interoperability between CAs can be solved.
- **Cost- Saving -** Online applications offer saving of time, cost and transportation which are important factors taken into account from the user point of view. Our system introduces secured online transactions to benefit users for doing business regardless of the region and time that can save other expenses such as travelling, accommodation, etc.
- **Convenience –** Buyer and Seller can communicate as well as do business online easily. Only a digital certificate which is stored in a secured, portable and removable device is required for user authentication and granting access to the system.

7 Conclusion and Future Work

We have presented the idea and implementation of PKI based multi-agent system including verification process of different PKI certificates on behalf of a human user. That solves PKI interoperability issues among different CAs. It also provides trust for online users which facilitates not only online commerce security but also to support startup entrepreneurs for secured trading by taking into consideration regional needs. With the use of our proposed system, user can identify each other easily which can strengthen business trust.

For improvement of our system, we need to consider including all applicable trust models. Currently, we have implemented a Hierarchical trust model as an example model for CA-CA interoperability. In order to apply it in the real world, we require creating a certificate database which must consists of all trust models [19] for the verification processes. Our future work includes the development of an adaptive model for checking certificate path validation of heterogeneous PKI integration to manipulate the shortest and best certification path by using software agents in the changing environments.

Acknowledgements. This research project has been supported by Asia Pacific Telecommunity (APT).

References

1. Adams, C., Lloyd, S.: Understanding PKI: Concept, Standards, and Deployment Considerations, 2nd edn. Addison-Wesley (2002)
2. More, V.N.: Authentication and Authorization Models. International Journal of Computer Science and Security (IJCSS) 5(1), 72–84 (2011)

3. Zhou, H.Q., Dai, S.H.: PKI-based E-Business Security System. In: The 3rd International Conference on Innovative Computing Information and Control, ICICIC 2008 (2008)
4. Liping, H., Lei, S.: Research on Trust Model of PKI. In: Fourth International Conference on Intelligent Computation Technology and Automation, pp. 232–235 (2011)
5. Achieving PKI Interoperability, Results of the JKS-IWG Interoperability project, Japan PKI Forum, Korea PKI Forum, PKI Forum Singapore (2002)
6. Lloyd, S., Fillingham, D., Lampard, R., Orlowski, S., Weigelt, J.: CA-CA Interoperability, White Paper (March 2001)
7. Guo, Z., Okuyama, T., Marion Jr., R.F.: A New Trust Model for PKI Interoperability. In: Proceedings of the Joint International Conference on Autonomic and Autonomous Systems and International Conference on Networking and Services, ICAS/ICNS 2005 (2005)
8. Finin, T., Fritzson, R., McKay, D., McEntire, R.: KQML as an agent communication language. In: Proceedings of the Third International Conference on Information and Knowledge Management, CIKM 1994, pp. 456–463 (1994)
9. He, Q., Sycara, K.P., Finin, T.W.: Personal Security Agent: KQML-based PKI. In: Proceedings of the Second International Conference on Autonomous Agents, AGENTS 1998, pp. 377–384 (1998)
10. Hu, Y.J., Tang, C.W.: Agent-Oriented Public Key Infrastructure for Multi-Agent E-service. In: Palade, V., Howlett, R.J., Jain, L. C. (eds.) KES 2003. LNCS, vol. 2773, pp. 1215–1221. Springer, Heidelberg (2003)
11. Hu, Y.J.: Trusted Agent-Mediated E-Commerce Transaction Services via Digital Certificate Management. *Electronic Commerce Research* 3, 221–243 (2003)
12. Fugkeaw, S., Manpanpanich, P., Juntapremjitt, S.: Multi-Application Authentication based on Multi-Agent System. *IAENG International Journal of Computer Science* J 33(2), 1316–1321 (2007)
13. Fugkeaw, S., Manpanpanich, P., Juntapremjitt, S.: A Robust Sign-On Model based on Multi-Agent System and PKI. In: Proceedings of the Sixth International Conference on Networking, ICN 2007 (2007)
14. Randy, C.M., Joseph, G.T.: E-Commerce Security Issues. In: Proceedings of the 35th Hawaii International Conference on System Sciences (2002)
15. Zhang, Z., Zhang, C.: Basics of Agents and Multi-agent Systems. In: Zhang, Z., Zhang, C. (eds.) *Agent-Based Hybrid Intelligent Systems*. LNCS (LNAI), vol. 2938, pp. 29–39. Springer, Heidelberg (2004)
16. Yannis, L., Finin, T., Yun, P.: Agent Communication Languages: The Current Land-scape. *IEEE Intelligent System* 14(2), 45–52 (1999)
17. Foundation for Intelligent Physical Agents: FIPA specifications, <http://www.fipa.org/> (accessed October 31, 2012)
18. Shimaoka, M., Hastings, N., Nielsen, R.: Network Working Group Request for Comments: 5217 Category: Informational, <http://www.ietf.org/rfc/rfc5217.txt> (accessed November 1, 2012)
19. Perlman, R.: An Overview of PKI Trust Models. *IEEE Network*, 38–43 (November/December 1999)