IJICTR International Journal of Information & Communication Technology Research

Volume 9 - Number 1- Winter 2017(25-32)

A Framework to Create a Certificate for e-Commerce Secure Transaction Protocol

Nasrin Alishirvani
Department of engineering, Payame Noor university
Tehran, Iran
n_alishirvani@ pnu.ac.ir

Received: November 16, 2016- Accepted: March 12, 2017

Abstract—**The development of e-commerce requires security to win the confidence of its stakeholders. Among the common protocols to establish safe financial transactions, Secure Electronic Transaction (SET) protocol has more security providing a safe protocol of payments at the level of the communication network between the buyers, sellers, banks and payment gates. In this protocol, all participants in the transaction should receive Certificate Authority (CA) identity. This paper analyzes the secure communication solutions and variety secure communication contracts for financial transactions. Then, architecture is presented to establish a web-based Certificate Authority (CA) identity for elements of Secure Electronic Transaction (SET) protocol and its implementation is described. The presented Certificate Authority (CA) identity in the article can process the requests of entities for online processing and transmit them through Hypertext Transfer Protocol (HTTP).**

Keywords: Component, Secure Transaction Protocol; Certificate Authority; Secure Electronic Transaction; Payment Gateway; Public Key Infrastructure

I. INTRODUCTION

E-commerce has reached an important place by Introducing information technology in the world and development of the Internet. However, what prevents the rapid growth of the business is consumer perception of security weaknesses on the network. As more payment methods are via credit cards, customers fear from the disclosure of their credit card information.

At the present, Security of financial transactions is supplied by secure communication protocols, especially ones such as SSL / TLS and SET [1]. SSL / TLS protocol is used in wider extent due to its simplicity, while the security of SET protocol is higher than the other one.

SET provides a secure payment protocol in the communication network between the buyer, the seller, the bank, and the payment gateway. In The SET protocol; all participating parties in the transaction must receive a certificate from the CA identity center. The position of this protocol in the protocol stack of TCP / IP is demonstrated in the Fig. 1 [1, 2, and 15].

SET is a set of algorithms and protocols that all are under specific procedure and protocol which enables users to make transactions via a public network such as the Internet. Therefore, to design and implement of SET protocol, identifying and studying of these algorithms,

SET	
HTTP	SMTP
TCP	
IP	

Fig. 1: Contractual Position of SET in the Stack of TCP / IP Protocol

and how to use them is essential. In this paper, secure communication solutions for financial transactions are investigated, secure communication protocols, including SET, SSL / TLS, IPSec, PGP, etc. are also analyzed.

In the end, architecture for establishing the identity certificate authority for payment gateway, on the basis of SET protocol is proposed.

According to proposed framework, CA Server is in the network for online in order to provide the security in the center from the invalid IP addresses using a three-layer firewall and NAT router and Roll located at the ISP to provide security between different components of SSL protocol**.**

II. AN OVERVIEW OF THE PAST LITERATURE

So far, lots of works have been done on the design and implementation of PKI. Some of these are available for free on the Internet and some are commercial products [3], including PyCA, OpenCA, Entrust / PKI and IBM Registry. Among them two free cases and two commercial ones are discussed as follows:

- *PyCA*: It is a set of CGI1 scripts that provides the interface between World Wide Web pages (WWW) and identity certificate authority. Scripts have been written in Python. That is why they were named pyCA. pyCA only implements a center of identity certificate and it is not accounted as PKI. Therefore, it does not maintain private keys of individuals and users are responsible for backing up their private key and their certificate [4].
- *OpenCA*: OpenCA is a common effort to create a public key infrastructure. It can be considered as reinventing pyCA in terms of programming but the difference is that its scripts are written in Perl. OpenCA uses OpenSSL as the underlying structure [4, 5].
- *Entrust/PKI*: Family of Entrust company products presents a solution for Public key infrastructure that are needed for e-commerce. This solution includes Cryptography- Based Services and digital signature.
  Entrust/Commerce CA is a product of Entrust to issue certificates for terminating entity. To do this, it receives certificate from higher certificate identity authority in the hierarchy of SET [6, 7].
- *IBM Registry*: IBM Registry is part of Net commerce product of IBM company that plays the role of the center of identity certificate in SET protocol. IBM Registry can be used on different machines as distinct identity certificate authorities(CA's). several CA's can be also run simultaneously on a machine [8].

III.. SECURE TRANSACTION PROTOCOL

With the introduction of information technology in the world and the Internet, E-commerce has reached an important position. One of the principles of e-commerce transactions is secure transaction, secure transactions over the network specially Internet requires high security, As sending data and financial information such as credit card numbers, account numbers, sending confidential financial information, codes, passwords and thousands of confidential pieces of information brings about much concern and this is a Justified reason for the significant importance of methods of providing security and different types of secure payment systems[9999].

So far, many protocols have been proposed as secure transaction protocols that only have one or a few features of secure transaction protocols. Some Examples of these are protocols of [10]: PGP, PEM, S/MIME, IPSEC, SSL, STP, and SET are examined.

A. *Pretty Good Privacy (PGP)*

PGP is the service of confidentiality and authentication for e-mail and file storage applications. Sending Public key is done by identity authentication that its transmission is physically impossible on the network. Sometimes it is electronically transferred or endorsed by telephone [11].

Another method is transferring by a trusted individual who has the public key. for instance public key of user A is signed by recognized and trusted user B and is sent to the user C or the transfer is done by the CA .however public key of individuals are not identified in this way but these CAs are used as accumulator [12].

B. Privacy-Enhanced Mail(PEM)

PEM is one of the algorithms that were created for e-mail security but it was not successful, and it is used rarely to send e-mail nowadays, due to the following reasons:

• PEM uses 56-bit DES encryption which is not a strong cryptography algorithm.

• Also, all the messages were signed in PEM and the signature was situated outside the encrypted message

[1] CGI stands for Common Gateway Interface. it is a part of the Web server that provides a feature so that in case of running a program on the server side, its output is displayed for user who is connected to the server through the web page.

and it was not necessary to decode message in order to find signer.

C. Secure Multipurpose Internet Mail (S/MIME)

S / MIME Protocol, is used for secure e-mail. It can be implemented in each automatic transmission mechanism which supports MIME (like HTTP); it uses the security services and requires no user interaction [12].

D. SSL (Secure Socket Layer)

SSL is a solution to communicate between a server and a client securely. The benefit of using this security protocol is taking advantage of its embedded security for securing Non-secure protocols of application layer such as HTTP, LDAP, IMAP, etc. Based on it, the encryption algorithms are applied on raw data which are supposed to pass through Non-secure communication channel as internet and data confidentiality during transmission channel is ensured [1, 13].

In other words, a company that is competent to issue and award of SSL digital certificates, issues special server and client certificates for each of the two sides that are supposed to have secure inter-networks communications, And using its own authentication mechanisms, affirms the identity of each of the parties to the opposite side. Moreover, it should ensure that if information is stolen while being transmitted, it should not be understandable and usable for robber because of using of encryption algorithms and asymmetric and symmetric encryption keys.

E. IPSec (Internet Security Protocol)

IPSec is not the general security architecture for the Internet but a developed protocol on IP protocol which has been provided for IP security. This protocol is widely used in virtual private networks (VPN) in offices related to a company or organization and essentially is implemented in establishing a secure connection between two or more organizations. IPSec uses two protocols of AH and ESP for more confidence on authentication, data integrity and confidentiality . The protocol can establish security at the network layer and in higher layer protocols in Transport state. The main objective of IPSec is augmenting security mechanisms ToIPv4 and IPv6 in order to provide required security for users.

F. SET (Secure Electronic Transaction)

Secure Electronic Transaction (SET) is a security protocol that was developed by Visa and Master Card. Unlike SSL which is an all-purpose system for encrypted communications, SET is only for transactions of credit card between buyer and seller.

SET protocol provides all the facilities supported by SSL. In addition, SET prevents awareness of seller from the buyer's credit card number and only presents it to the bank that issues the credit card.
Business needs [14] which are met by the SET [15, 16, and 17] include:

Confidentiality, data integrity, identification and cross-operational capability, in this section, these needs and how they are met by the SET are taken into account [18].

Confidentiality: payment details and how it works should not be visible for someone who secretly monitors this process. Confidentiality is guaranteed by the use of message encryption. Including:

- Symmetric-key cryptography such as: DES, 3DES, RC2, RC5
- Public-key cryptography, like : RSA, Diffie-Hellman, Digital Signature, Message Digest

Identification: in SET Protocol, identity of all parties involved in the transaction should be assured. Confirmation is guaranteed by the use of digital signatures and authentication. SET protocol implements certificates of X.509 V3[11] and RSA signatures for identification of parties.

Data integrity: it should be assured that data received in the SET transaction is exactly the same as sent data . The evolution is guaranteed using digital signatures. To prevent distortion of the message in the route, SET uses digital RSA signature and SHA-1Hash and in some cases HMAC and SHA-1 for ensure data integrity assurance.

Cross- operational capability: SET specifications must ensure that it works in different hardware and software platforms. The ability to exchange information is guaranteed by using the message templates and specific protocols. Content and message encryption is in a standard form. SET utilizes ASN.1 and DER for this purpose. It uses the standard of PKCS # 7 to encapsulate the messages.

IV. THE PROPOSED CERTIFICATE AUTHORITY (CA)

A. Tasks of the suggested CA identity

The tasks of CA identity in the SET protocol include: issuing certifications, canceling certificates, and maintenance of certificates, maintenance of lists of denial of certifications, and Brand CRL[2] Identifier (BCI). Since in the protocol, private key entities in the end are not sent to the CA identity, it does not take responsibility for private key entities in the end. And each entity is only responsible for maintenance of its own private key (s).

In SET protocol, tasks of CA identity center of the card holder are similar to the CA identity centers of seller

[2] Certificate Revocation List

and payment gateway. Both CA identity centers of card holder and seller are responsible for issuing certifications, canceling certificates and maintenance of certificates, maintenance lists of denial of certifications, and BCI.

- In the proposed model, the CA identity center of payment gateway takes responsibility for issuing and keeping certificates, lists of denial of certifications and BCI. We also have certified payment gateway falsified, unlike the other end entities.

B. *Features of the identity certificate authority of proposed payment gateway*

In this architecture both valid and invalid IPs are used to enhance the security. Unlike the usual way, valid IP in local network of CA server is not set on any computer and invalid IP range within one class is used in all networked computers and other devices on the network, and also the router which is connected to the ISP suffering and wishes of a class.

To receive sent packets to this network with a valid address, a rule is used which has been programmed in the router located at the service-provider. Therefore, packets with the destination address (Valid Address) and Address of origin (Any Address) are sent to the local network. A firewall with three layers at the local network gateway is situated with the possibility NAT.

Activities which are done at any layer of the firewall are as the following:

- *Access Control*

The first layer firewall: To determine the prohibited packages (black) and delete them. Header fields of IP packet are analyzed in the first layer.

Source address: some of the machines inside or outside the network do not have the right to send the packet, therefore their packet are deleted upon arrival at the firewall.

Destination address: some of the machines inside or outside the network do not have the right to receive the packet, therefore their packet are deleted upon arrival at the firewall. Invalid IP address in transmission mode in case of sending packet to the local network is any IP except valid IP of local area network.

The second layer of firewall: closing some ports of some services, such as Telnet, FTP, etc.

In the second layer, header fields of transport layer are examined. Due to the fact that Port number of the process of source and destination are the known standard port numbers, only packets with ports numbers that CA Server will listen to them are passed and the rest of the packets are deleted. However other ports can be closed except intended ports of CA Server.

- *Filtering*

The third layer of firewall:

Analyzing the outcome of a web page text, E-mail, and so on, due to the fact that protection in the third layer is made based on type of service and the application, packets are controlled by controlling standard protocol of X.509.

For example, a request that its Issuer Name field is not same as the name of our CA or other acceptable CA is thrown away. Therefore in this level, processing volume is high.

- Network Address Translation (NAT)

  After the operation of Access Control and Filtering, valid address of CA Server must be translated to invalid address in the internal network. Thus the packets passed the NAT and the reverse operation is done for traffic outside the internal network.
- To enhance the security in this architecture, different parts of the local network are associated together via native SSL protocol; manipulated SSL.
- In the proposed center of certificate for communicating between users and identity certificate authority, HTTP protocol in secure form of HTTPs is used.
- Ability to request certificate online exists in offered identity certificate authority where CA is maintained on-line and is capable of processing requests online.
- LDAP directories are implemented to publish and retrieve certificates and revocation lists of certificate. This directory enables a secure connection and information is securely exchanged between this directory and the CA.
- The identity certificate authority of Payment Gateway is responsible for issuing and maintenance of certificates and certificate revocation lists and BCI . moreover, against other terminating entities, Certificate Revocation of Payment Gateway is also available.

C. Architecture of proposed authentication center

Considering the duties of identity authentication centers of card holder, seller and payment gateways of identity authentication centers is composed from the following components Fig. 2:

CA Server: It plays the role of identity Certificate Authority. All requests for issuing certificate is given to this server. If CA Server requires identification of any request, sends a message to the RA Server.

RA Server: It is responsible for identification of individuals. When RA Server receives request of entity identification, identifies that one using the information in its database identification And announces the result is to the CA Server.

LDAP Repository: LDAP directory is used for maintaining certificates and certificate revocation lists. CA Server certificate places certificates and received certificate revocation lists from higher CAs in the hierarchy of SET as well as certificates and certificate revocation lists issued by itself in LDAP directory.

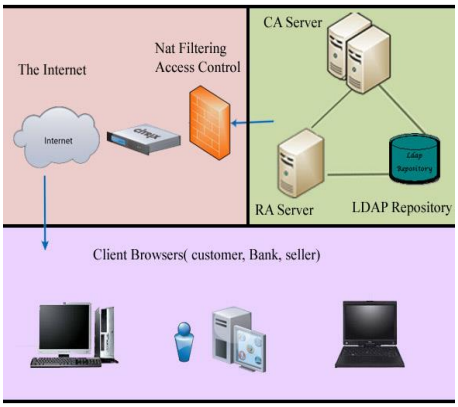

Fig. 2: Architecture of the Proposed Identity Certificate Authority

D. The Process of Receiving Certificate by Users in the Proposed Architecture

The certificate process certificate for seller and receiver is very similar to this process for the cards holders, but there are significant differences that arising from the nature of the parties involved in the transaction that include:

- The seller has two pairs of keys (A pair for signs and another pair for key exchanges).
- The certificate process for card holders will probably perform on the Internet and on-line entirely, while in the case of seller there is always offline validation too.

In this paper the certification process for card holder is explained in details:

The card holder begins the registration.
The card holder is connected to the RA web server through its browser and requests for awakening message. By receiving the awakening message and informing of
the URLs needed to connect to the CA, the certificate request process will begin. The card holder sends the beginning message through HTTPs protocol to the RA server.

- **RA server sends the response.**
RA server receives the beginning request of the card holder and after investigation sends it to the CA server. CA server also sends both itself certificates for the public signature key and key exchange of public key. These certificates will be used to protect payment card account number on the request for registration form.
- **The card holder requests the registration form.**
Identity authentication center needs some details to confirm that cardholder is the same person who claimed. The card holder receives the beginning response message from RA server and measures the accuracy of the certificates by examining the chain of trust to the roots. The accuracy of identity authentication center's sign measured by performing the beginning response (as shown in fig. 3 through a hash function and a summary message is created. Digital signature is decrypted by using public signature key of Identity authentication center and its results are compared locally to the obtained abstract message. If they are the same, the accuracy of Identity authentication center's response is guaranteed.
The card holder enters the credit card account number and the card holder's software creates a registration form. Request a registration form is encrypted by the symmetric key (K1 in Figure 3) that is randomly created. These symmetric key and card holder's account number are encrypted by key exchange of public key and a digital package is created.

Identity authentication center sends registration form
Registration form is transmitted emptily, but Identity authentication center signs the message in order to the card holder be able to ensure of its validity. RA server receives the registration form, since previously identification has been conducted sends the digital package to the CA server.CA server decrypts the digital package by key exchange of private key of identity authentication center in order to achieve card holder account number and symmetric key. Symmetric key is used to achieve the request of the registration form (via decryption of encrypted registration form). Identity authentication center determines the appropriate

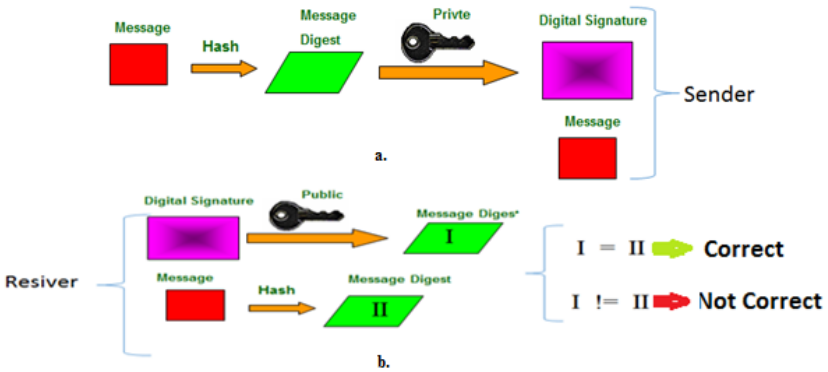

Fig 3. Controlling of Verifying of the Received Identity Certificate

registration form for this user and a digital signature is created (as shown in Fig. 3 - a). Identity authentication center sends the registration form, digital signature and certificate of Identity authentication center (containing the public signature key) to the card holder.

Card holder requests the certification

The card holder's software provides the request form and creates a request message. The card holder receives message of registration form from the RA server and measures the accuracy of certificates by examining the chain of trust to the root and based on fig. 3 the accuracy of message are guaranteed. The card holder's software creates a pair of keys and stores them safely then fills out the registration form and sent it along with a random number in order to create a certification by identity authentication center. It creates a certificate request message by using the information in filled registration form and random number. Certificate request and registration form are encrypted by private signature key of card holder (as shown in Fig. 3) and a digital signature is created. The card holder creates two keys accidentally (we call them symmetric key (1) and symmetric key (2)). The card holder catches registration form, certificate request, digital signature, public signature key of card holder and the symmetric key (1) and encrypts them by using symmetric key (2). Symmetric key (2), the card holder's account information, history of accurateness and random number encrypted by key exchange of public key of identity authentication center and a digital package is created. Digital package and encrypted message are sent to the RA server.

Identity authentication center receives the request

Now Identity authentication center should decrypt the message sent by the card holder and process the registration request. Digital package is decrypted by using key exchange of private key of identity authentication center in order to reveal Symmetric key (2), account information and random number. Encrypted message is decrypted by using a symmetric key (2) in order to the public signature key card holder, the symmetric key (1), certificate request, registration form, and digital signature be achieved. The authenticity of the signature of the card holder is guaranteed by performing certificate request and registration form (as shown in Fig. 3) and by using public signature key of card holders. Now Identity authentication center reviews the certificate request by verification of card holder's account and details of registration form in comparison with information of trademark database. If the information is valid, RA server sends its request to the CA server. In CA server the following steps are passed.

First, identity authentication center creates a random number that combined with the random number that created by the card holder's software in order to create a serial number. Account number, expiration date and serial number are encrypted by using one-way hash algorithm. The obtained result is inserted in card holder's certification. Then the certification is signed digitally by identity authentication center and by using the private signature key. The certification placed in a certification response message which is signed by passing it through a hash function. The abstract of message that created in this way is encrypted by private signing key of identity authentication center that it will bring a digital signature. Identity authentication center encrypts the digital signature and response of certification that contains a random number (that created by identity authentication center) and other information (such as logo trademark), with a symmetric key (1) that the card holder receives. The obtained message, certification of identity authentication center and the certification of card holder are sent to the card holder.

Card holders will receive a certificate

The card holder reviews the accuracy of received certification and stores it. The card holder reviews the accuracy of certification by examining the chain of trust to the root. The encrypted certification response is decrypted by using symmetric key (1) in order to obtain the certification response and digital signature. The card holder's software now recognizes the symmetric key (1) since created it in first place. It combines the random number sent in the registration form with the random number in the certification response in order to obtain the serial number. This number is stored for use with a certificate.

Accuracy of received signature of identity authentication center is guaranteed by performing the certification response (Fig. 3) and by using public signing key of identity authentication center. The card holder's software stores the certification in a safe place on disk or another intermediary in order to use it in the future. The card holder can buy now. This process is shown in Figure 4

V. Evaluation of Performance

Parameters considered in the assessment of identity certificate authority include: Throughput and average response time for requests of opening, registration forms and certificate. Throughput is referred to the number of requests processed per unit of time. The Throughput chart of identity CA based on the number of concurrent Applicants is shown in Fig. 5. throughput of the center is slightly reduced by increasing number of applicants.

In contrast to other servers, CPU time is wasted here and efficiency is being reduced by declining the number of clients while the performance is being boosted by increasing of demands.

In This server, such state does not exist because the efficiency is not augmented by increasing of clients due to cryptographic operations and filling of CPU time.Average response time of requests is referred to the average time servers take in order to respond to each question. Fig. 6 demonstrates Average response time of certificate request form.

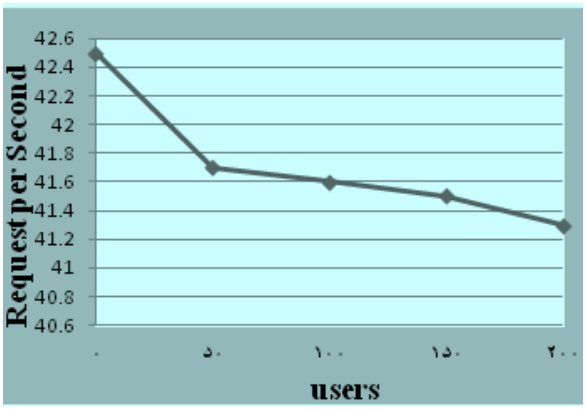

Fig. 5: Throughput of Identity CA

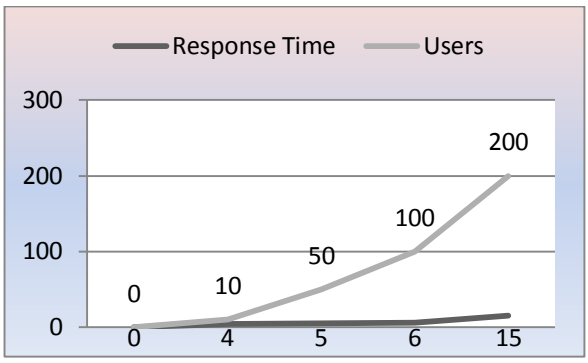

Fig. 6: Average Response Time of Certificate Request Form

VI. THE COMPARISON OF THE PROPOSED ARCHITECTURE WITH PRESENTED ARCHITECTURES

PyCA architecture uses a pair of keys, while the SET protocol requires two pairs. In this architecture, the private system of CA is kept is offline. Lots of messages

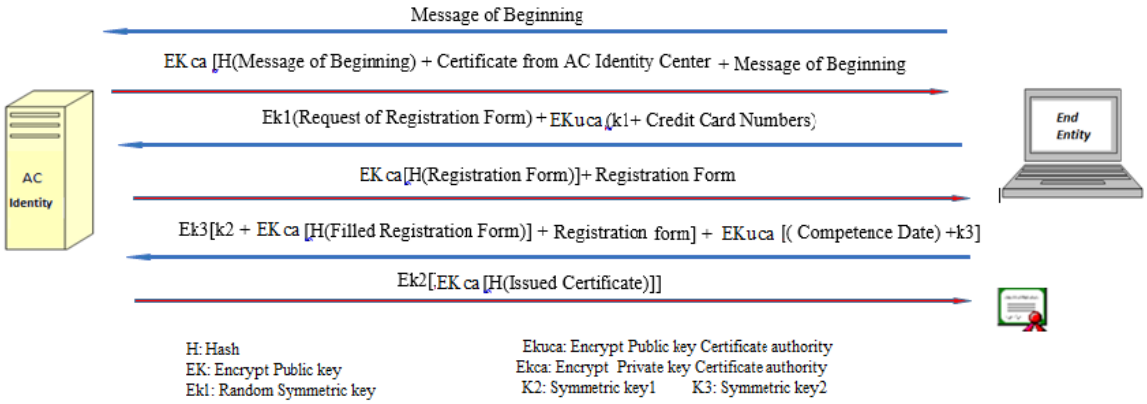

Fig. 4: The Process of Receiving Certificate by Card holder in the Proposed Architecture

to users in The SET protocol is identity signed by the certificate authority. This would be in conflict with the lack of availability of CA private system. In this architecture, much work has not been done for the identity of users.CA server in OpenCA architecture is kept as offline and various stages of Certifying requires user interaction, which is accounted as an architectural weakness. This architecture places a strong emphasis on the identity of individuals. OpenCA is capable of publishing certificates and Certificate Revocation Lists in LDAP directory.Usability of the issued certificate by other identity certification authorities exists in the architecture. Therefore, it can be implemented for hierarchical model. The architecture of the certificate revocation list is used to declare the status of individuals.Architecture of Entrust / PKI does not have previously expressed weaknesses. Entrust / Commerce CA Product of this company is written specifically for SET protocol. Entrust / Commerce CA just supports some identity certificate authorities of the SET protocol.IBM Registry is part of the Net Commerce product of IBM Company and purely has been written for SET protocol. This production also supports only some identity centers in The SET protocol.As the features of the proposed identity center mentioned in the article, Comparison between the proposed identity CA and existing identity centers (commercial and noncommercial ones) in terms of capabilities has been conducted in Fig 7.

Open source	High rate of	Identification of Users	Two pairs of keys	online CA	
✓	✓	✗	✗	✗	PyCA
✓	✗	✓	✗	✗	OpenCA
✗	✓	✓	✓	✓	Entrust/PKI
✗	✓	✓	✓	✓	IBM Registery
✓	✓	✓	✓	✓	The proposed architecture

Figure 7: Comparison of the Proposed Architecture with Available Identity Certificate Authorities

VII. Conclusion

In this paper, secure transaction protocols and their features were investigated. A number of commercial and non-commercial identity certificate authorities were discussed and according to the SET protocol requirements of an identity certificate center devoted specifically for, this Protocol, an identity certificate authority was presented.The proposed identity certificate authority is capable of processing entities Requests online. And requests are sent and received through the HTTP protocol. As the CA server is online on the network, invalid IP addresses, three-layer firewall, NAT and router rule located at the ISP are used to establish security in the identity certificate authority. SSL protocol has been implemented between different components to provide security.

References

[1] Angeliki Vos, Catherine Marinagi, Panagiotis Trivellas,Niclas Eberhagen, Christos kourlas, Georgios Giannakopoulos,'Risk Reduction Strategies in Online Shopping: E-trust perspective', Procedia - Social and Behavioral Sciences 147 (2014) 418 – 423

[2] Zhang Boping, Shang Shiyu, "An Improved SET Protocol", Proceedings of the 2009 International Symposium on Information Processing (ISIP'09), Huangshan, P. R. China, August 21-23, 2009, pp. 267-272

[3] Booz•Allen & Hamilton , Public Key Infrastructure (PKI) X.509 Certificate and CRL Extensions Profile,Elkridge Landing RoadLinthicum, Maryland, October 12, 2005

[4] Symeon (Simos) Xenitellis,OpenCA Team, A Guide to PKIs and Open–SourceImplementations, Version 2.4.6 Edition, published by the Free Software Foundation; July 2000

[5] The Open Group Certified Architect (Open CA) Program, Conformance Requirements (Multi-Level) Version 1.1 October 2014

[6] Marc Laroche, Common Criteria Evaluation for a Trusted Entrust/PKI™,Version: 2.0, March 2000

[7] Marc Laroche, Darryl Stal, Security Target,Entrust/RA 5.0, Entrust Technologies Limited ,Version: 0.9,, February 28, 1999

[8] IBM Corporation, Secure Electronic Transactions: Credit Card Payment on the Web in Theory and Practice, IBM Corporation, International Technical Support Organization, June 1997.

[9] Raghav Gautam, Sukhwinder Singh, " Network Security Issues in e-Commerce ", International Journal of Advanced Research in Computer Science and Software Engineering", Volume 4, Issue 3, March 2014

[10] Gordon Agnew, Secure Electronic Transactions:Overview, Capabilities, and Current Status,springer,2003,IX,p 334

[11] A.D.N.M. Fernando, H.M.P.M.B. Herath, M.L.R.K. Senarathne, D.P. Brandiwatta, T. Kiroshan, M.P.Madushika, P.A.D.A. Senarathne, Mr. Dhishan Dharmmearatchi, " Biometric Encryption: E-Commerce Security Using Cryptography Techniques", International Journal of Scientific and Research Publications, Volume 6, Issue 10, October 2016

[12] Glenn Benson, "Portable Security Transaction Protocol", Computer Networks Volume 51, Issue 3 , 21 February 2007, Pages 751-766

[13] Omariba, Z.B., Masese, N.B., & Wanyembi, G. Security and Privacy of Electronic Banking. International Journal of Computer Science Issues, Vol. 9, Issue 4, No 3,432-446July 2012

[14] Deepak Kumar, Nivesh Goyal ," Security Issues in M-Commerce for Online Transaction", 978-1-5090-1489-7/16/$31.00 ©2016 IEEE

[15] Xu Yong and Liu Jindi (2010), 'Electronic Payment System De-sign Based on SET and TTP,' 2010 International Conference on EBusinessand and E-Government, Guang-zhou, 7-9 May 2010, pp. 275-278.

[16] K.Swathi, Reshmy,'NETWORK SECURITY IN E-BANKING', International Journal of Advances in Engineering Research (IJAER) 2014, Vol. No. 8, Issue No. IV, Oct

[17] Hassan M. Elkamchouchi, Eman F. Abu Elkhair and Yasmine Abouelseoud, 'AN IMPROVEMENT TO THE SET PROTOCOL BASED ON SIGNCRYPTION', June 2013, International Journal on Cryptography and Information Security (IJCIS), Vol.3, No. 2,

[18] Nasrin ALISHIRVANI, Batool MORTAZAVI," Guaranteeing of trust and security in e-commerce by means of improved SET protocol", Bulletin de la Société Royale des Sciences de Liège, Vol. 85, 2016, p. 1136 – 1147

Nasrin Alishirvani was born in Tehran, Iran, in 1974. she is currently faculty member at the Department of engineering, Payame Noor university, She authored the Computer networks 2 book, She has published a number of research papers in international scientific journals and conference proceedings.