INFORMATION SECURITY: MUTUAL AUTHENTICATION IN E-COMMERCE

S.H. Von Solms
Department of Computer Science
Rand Afrikaans University
PO Box 524, AUCKLAND PARK, 2006
South Africa
Tel: +27 11 489-2847 Fax: *+27 11 489-2138*
basie@rkwrau.ac.za

M.V.Kisimov
Department of Computer Science
Rand Afrikaans University
Johannesburg, South Africa
Tel +27 11 673-0163 Fax +27 11 673-0163
kisimov@yahoo.com

Abstract: Information Security is ever increasingly becoming an important topic when it comes to network communications. This greatly concerns areas of electronic commerce, especially online shopping and money transfers. This paper outlines a methodology for securing electronic communication between e-Merchants and online shoppers. The methodology is based on a simple hierarchy of a trusted third party and communicating hosts. The paper further explains how the new methodology avoids e-commerce pitfalls of current technologies and presents an approach for securing currently unsecured online shoppers, in the process of making them capable of performing safe and secure network transactions.

Keywords: Certification Authority, Authentication, Guideline, Security, Digital Certificates, Encryption, Asymmetric Cryptography, Digital Signature.

1. INTRODUCTION

In an ever-improving technological world, e-commerce is becoming an increasingly popular a tool for communication, business and analysis. Consequently the value of information being transmitted and its preservation is of high importance to its owner. This paper presents a new methodology, based on current technologies, which avoids security pitfalls to which current e-commerce standards are prone. This methodology deals with outlining a clear process for securing an average online shopper, with the necessary attributes needed for performing a safe online transaction. Further it defines an authentication process for verification of communicating parties' identities, using a trusted third party in the form of a Certification Authority (CA). As a result this methodology provides a legal process for creating nonrepudiation of performed transactions, which can be used in verifying the origin and the occurrence of a transaction.

1.1 Outline

Section two of this document looks at background work done to improve authentication between communicating parties as well as focusing on current electronic commerce problems and security loopholes. Section three of the document outlines the proposed methodology, which is the main focus of this document. Finally section four serves as a logical end to the document summarizing the important points made throughout.

2. BACKGROUND AND SECURITY PROTOCOLS

This section presents certain pitfalls of current e-commerce strategies and standards, in terms of security, customer satisfaction, authentication and technological standards. It will further present certain security weaknesses of the SSL protocol, which can be exploited by malicious parties. The points discussed here, present an obstacle to companies and individuals in establishing proper standards for electronic commerce and information security.

2.1 Customer Satisfaction

In a recently conducted study [PWC 98], statistics vital and worrying to corporations conducting business over the Internet as well as to online shoppers have emerged. The study showed that 60 percent of initiated online transactions are abandoned due to lack of online support, necessary security measures and lack of a standardised legal process for completing the online transactions. The ratio of completed to initiated transactions should be very discouraging to online merchants. Problems arising due to complex techniques and unproven technologies, often lead potential customers dropping transactions midway through and searching for different online merchants. E-Merchants, who present customers with long and extended processes for completing transactions, are usually the ones to suffer from lost business [PWC 98]. Security is of high concern to as many as 58 percent of online shoppers and only fewer than 10 percent of online shoppers are not concerned with security while performing a sensitive Internet transaction.

2.2 Online Digital Certificate Verification

Research performed by the authors reveals that many commercial products used for online transactions, which employs asymmetric cryptography and Digital Certificates (DCs) as method of encryption and authentication, over unprotected networks, do not provide methodology for online verification of these DCs. The need for such verification is based on the fact that Digital Certificates can be tampered with, corresponding private keys can be lost or compromised. This can cause information secured with these keys, to be compromised and to become volatile to malicious security attacks. Currently existing Certification Authorities (CAs) and PKIs such as VeriSign and Entrust [CTNS 00], [VS 01] implement special Certificate Revocation Lists (CRLs) [BPKIC 01], which hold a list of certificates, which are registered or issued by the CA or PKI. These lists represent DCs, which have been compromised in any manner. A verification of the DCs in use between communicating parties, in the issuing CA's CRL will confirm that in fact, these certificates have not been reported to be compromised. This can serve as a verification of the security of the data being transmitted. Such verification is not a property of any of the commercial products, which concern themselves with digital, network-based communication. Taking the problem further, if a certain certificate has been compromised, but the tampering has gone undetected to anyone, this certificate would not be reported to the CA and consequently not listed in the CA's CRL. This would leave any communication employing this DC compromised.

2.3 Authentication of online customers

Credit card fraud is a common occurrence for e-Merchants [PWC 98]. Reasons for fraud vary from lost credit cards, falsely generated credit information and duplicated or stolen credit cards being passed to the Merchant. Currently true authentication of the online shoppers is not always possible. Very few commercial or other products are in place, which deal with authentication of communicating parties over an open network. The latest version of the SSL protocol [SSL 96] provides for the possibility of such authentication. This however is not a prerequisite for the functionality of SSL. This leaves an opportunity for fraud on the side of a malicious online shopper. The fact that the e-Merchant cannot certainly authenticate a client, is enough for attempts at credit card fraud to be a persisting problem. Resulting statistics [PWC 98] show that credit verification systems are not advanced enough, resulting in false credit information being accepted as genuine. This inexorably hurts financially any e-Merchant having accepted fraudulent information as well as hurting unsuspecting people, whose credit information is in the possession of a malicious party.

2.4 Security Protocol Characteristics and Exploits

Current e-commerce trends [PWC 98] for securing Internet transactions reveal that the SSL protocol is seen and used by e-Merchants as the more secure alternative in providing a secure channel for transmission of sensitive information between online shoppers and electronic Merchants. The set of procedures provided by SSL allow for different options for securing and authenticating communicating parties [SSL 96]. There are three different options, which the protocol supports for the purpose of authentication:

- Anonymous communication; no authentication of any of the communicating parties.
- Server authentication; only the digital certificate of the server (e-Merchant) is transmitted to the client for authentication.
- Complete authentication; there is a mutual exchange of certificates between client and server.

The second and third option as listed above of the authentication process provide for a relatively sound structure for verification of e-Merchant (server) identification. The weakest option of the three listed is the anonymous connection between communicating parties, where no certificates are exchanged and thus no authentication is possible. This scenario is vulnerable to man in the middle attacks [SSL 96]. This can present a great cause for concern to any online shopper, as this weakness, if exploited

properly can result in unsuspecting person's or entity's, credit information to be transmitted to a malicious third party, pretending to be a genuine e-Merchant [SON 97].

2.5 Secure Electronic Transaction (SET)

Based on the development of new technology such as smart cards, a new security protocols SET has emerged, whose purpose is to provide authentication and secure transactions between communicating parties [SET 97]. The main goal of SET is to allow specific cardholders and properly equipped web merchants to perform business transactions over an open and unprotected network. Such transactions, similar to many security payment protocols, are based on use of a set of cryptographic techniques, for the purpose of secure communication. The protocol further introduces a new approach to digital signatures, although it does not introduce any new algorithms or technologies. This approach sees the concept of dual signatures. This is done with the purpose of encapsulating an eventual payment to a merchant directly to the client's bank, as well with the purpose of creating an offer for goods or services to the merchant. If this offer is accepted, the merchant receives the full amount decided upon into his bank account, without being aware of the customers' credit particulars. In the same breath, the bank is not aware of the types of goods or services being purchased, or of their individual cost. This is all possible, with the existence of specific client and merchant side certificates. These are issued by each financial institution, which issues the credit smart card to clients and is in a relationship with the specific web merchant. The client certificate is stored on the client's smart card, but this certificate is optional and not compulsory. This coupled with the fact that not too many individuals are in the possession of a smart card reader, or in the case where they attempt to purchase goods or services online from a different form their own computer, this protocol, will not function properly in terms of authenticating the client as required by the protocol's functionality, thus presenting problems often encountered by web merchants. Such problems deal with trust in the funds and validity of the credit information provided, as well as the fact that the credit information may be valid, but stolen from its original owner.

2.6 Summary

This section presented certain security weaknesses and methodologies, which can be found in current e-commerce practices. The main concerns addressed here represent a low level of customer satisfaction of e-traders, based on poorly designed and implemented online trading practices, weak security

measures for transmission of sensitive information, as well as lack of standardised practices for electronic transactions.

3. PROPOSED MODEL

3.1 Introduction

The proposed model outlines solutions for the problems encountered and described in the previous section as well as adding some extra features, which improve the overall security of the model. The model presents a methodology called Trusted Third Party (TTP), for securing a totally unsecured client, willing to perform online purchases, the authentication of communicating parties during this online transaction, as well as a secure transmission of sensitive information between them in the process of completing the online purchase.

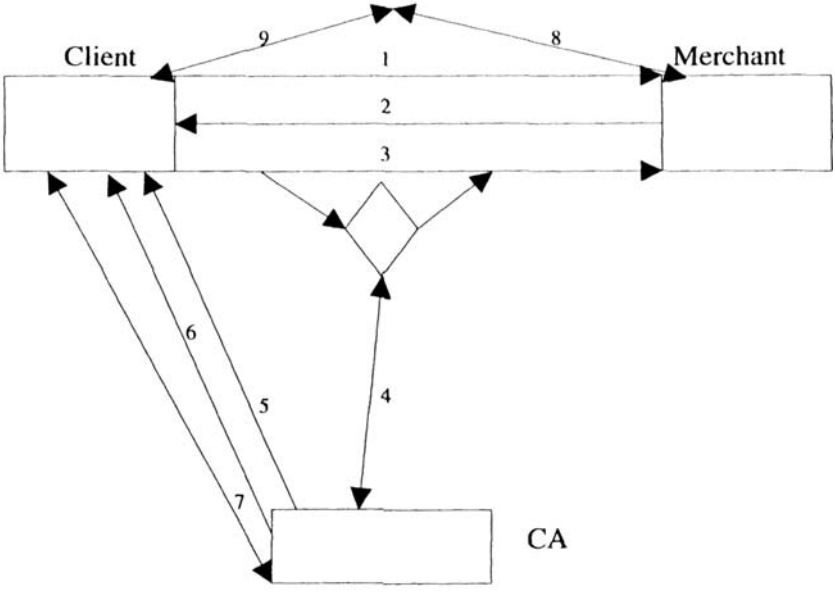

Fig 1.

3.2 Overview

The figure above describes the functionality of the Methodology presented here. An online transaction is usually initiated with an online shopper visiting

the desired e-Merchant's web site (step 1). At this point the Merchant's server initiates a SSL session as specified in [SSL 96], with the online shopper. Once the initial SSL handshake procedure is initiated and the Server DC is delivered to the Client, the Server requests similar DC from the Client (step 2). If the Client is not in a possession of such certificate (step 3), the SSL session with the Client is interrupted and the client is notified that he/she needs to perform certain steps in order for the transaction to be secured. If he does decide to take up these steps, the shopper is redirected to the trusted CA's web site (step 4), while his session with the Merchant remains frozen. At this point the root certificate of the trusted CA is delivered to the shopper (step 5), followed by a small application, which is too installed at the client's machine (step 6). Immediately after that a Java applet is delivered to the client (step 7), which communicates with the installed application from step 6 and generates two pairs of asymmetric keys, followed by the generation of corresponding DC. This completes the securing of the client and is followed by resumption of the frozen Merchant session. This sees a different Java applet delivered to the client (step 8) used for credit information gathering and its encryption by the client residing application, as well as its transmission to the Merchant (step 9). Steps 8 an 9 do not follow through from entity to entity. This is done with the purpose of representing multiple transmissions of data between clients and merchant, once a secure communication between the two has been established and the appropriate authentication has been performed on either side.

3.2.1 Trusted third party

Based on the principal of trust, the trusted third party does not participate in any online transactions. Its sole purpose is to provide means of authentication and encryption for other entities, in order for them to be able to perform secure transactions over an unprotected network. Such attributes are provided by Certification Authorities [BPKIC 01]. The trusted third party within this methodology will be referred to as *Master CA*. The Master CA, consistent with the requirements of a CA, has a root certificate. One difference, which is vital to this section, is to mention that the root certificate of the Master CA is not self-signed, which is generally the practice of most well known CAs, it however is cross certified by a third party CA, which does not belong or is connected in any way to the Master CA.

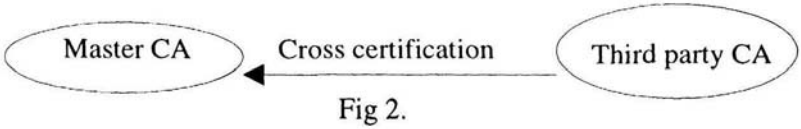

Fig 2.

3.2.2 E-Merchant

An e-Merchant is an online trader, providing sale of products or services. The Merchant requires payment in terms of a specific monetary currency, in return for his product or services. In most cases this payment is in the form of credit information, which is transmitted by the client to the Merchant. In order for the e-Merchant to be authenticated, he will need to have two Digital Certificates, holding the public keys for encryption and digital signature respectively. Intuitively, the private keys for those two corresponding public keys need to be in the possession of the Merchant and nobody else. The DCs are registered with the Master CA, with an appropriate chain of trust, and listed in this Master CA's Public Directory, if the Master CA itself has not issued them. The DCs need to be listed in the Master CA directory if not issued by the Mater CA, in order for the Master CA, serving as a point of trust, to be able to verify, the identity of the Merchant. The chain of trust to such a Digital Certificate needs to verifiable, in order for the Master CA to be able to trust its origin.

3.2.3 Online Shoppers (Clients)

These are people or entities, which wish to perform online transactions, in the form of purchases, from authentic e-Merchants. In order for an online shopper to be able to provide his or her sensitive credit information to the e-Merchant, he or she will require attributes similar to the Merchant's. These will be two pairs of public/private keys, for the purposes of digital signing of data and encryption respectively. The public key of each respective pair will need to be encapsulated in a Digital Certificate, which is either issued by the Master CA and thus signed by it, or is issued by any other CA with a verifiable chain of trust, and as with the e-Merchant scenario listed in the Master CA's Public Certificate Directory.

3.3 Initial Steps

The previous subsection described the minimum attributes required by two parties, in order for a secure communication to be established between them. The described scenario involved the introduction of a trusted third party, which does not take any part of any possible transactions involving an e-Merchant and an online shopper. Even though the online shopper and the e-Merchant are equipped with the necessary attributes to complete a secure online transaction, the two parties don't have a methodology in place, which will employ these attributes in a correct manner. Existing methodologies such as SSL have certain pitfalls, such as no online verification of DCs in

CRL, determining chain of trust of used certificates as well as guarantee of an existing standard for processing online transactions. Having said all that, most online shoppers are not equipped with any of the Listed minimum attributes. Shoppers are purely restricted by the use of an Internet Browser (IB) and their concern of security of the transaction.

3.4 Obtaining the Master CA's Root Digital Certificate.

Once the online shopper is redirected to the Master CA's web site, the CA's Server detects his Internet Browser's make. That done, the shopper is further redirected (the whole process is automated) to download the Master CA's Root DC, which is cross certified by the maker of the shopper's Internet Browser. This done, the shopper's Internet Browser verifies the digital signature of the cross certifying third party CA (not the Master CA). This is possible, because each Internet Browser comes with the root certificate of the maker of the IB. This coupled with the fact that the root certificate of the Master CA is cross certified by the private key of the maker of the online shopper's IB makes this verification possible. From this point onwards the following procedures become more automated.

3.4.1 The Master CA's root certificate

Following standard asymmetric cryptography techniques, in order for a Digital Certificate to be generated there needs to be a public key of a publid/private key pair encapsulated in it. The key pairs for the root certificate of the Master CA are generated using the standard RSA algorithm [PGP 95]. Use of other approved asymmetric algorithms can be equally as effective. The key length is of 2048 bits size. The private key of this pair is always kept with the Master CA. The public key is distributed to all known Internet Browser manufacturers, who based on it generate a Digital Certificate, which is signed with their own private key. Employing this technique the online shopper can be asserted that the received Master CA root certificate is indeed authentic and not fraudulent. Such approach can prove to be expensive, but it server to right purpose of secure transmission and identification of origin of transactions.

3.5 Background process

Once the Master CA's Root Certificate has been installed, any file or application signed with the private key of the Master CA will be guaranteed and be verifiable by the online shopper to be authentic and non malicious. This is used for the base of downloading a small application, which is

installed and run on the client's machine. The application runs as a background process to the IB and is active throughout the whole time the client's machine is powered on. This application brings with itself the root certificates of the major Certification Authorities from around the world. These certificates are not hard wired into the application and are exchangeable, once they expire or become compromised. The application has networking capabilities, which will be discussed in the following sections. As part of the installation process, the application gives security permission to Java applets to interact with this background process. At no time however will an applet be able to control the background process.

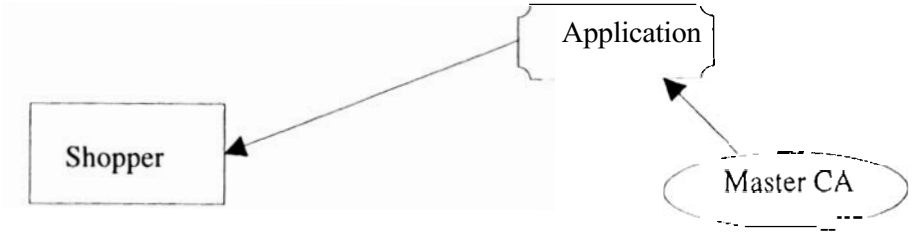

Fig 3.

The applet will simply be able to pass information to the process in the form of structured data.

3.6 Key pair generation

3.6.1 Review

The next step of the process sees the download of the application and its installation followed by continuation of the connection with the Master CA's server. After the installation procedure of the background process is complete, the client is redirected by the CA's server to download a Java applet.

3.6.2 Key generation and Digital Certificates

This applet is signed by the Master CA's private key. The purpose of this applet is to generate two pairs of keys using the RSA algorithm, or a similar asymmetric algorithm. These key pairs have the purpose of encryption and digital signing respectively. Once the applet is downloaded, its digital signature is verified by the IB. Following this, the two pairs of keys are generated. The public keys are passed to the background process, which signs them with the just generated signing private key, encrypts them with the public key of the Master CA, obtained from its certificate and passes

them back to the applet. The applet sends this encrypted information back to the Master CA, which decodes this data and verifies the digital signature. Digital Certificates are created, encapsulating these public keys. The certificates are listed in the Master CA's Public Directory as well as these DCs being sent back to the applet, which together with the corresponding private keys are passed to the background process, for the purpose of storage and further use.

3.6.3 Communication between applet and background process

The communication between the applet and the background process is possible due to the fact that the applet has security permissions to communicate with this process. Before any communication between background process and applet is performed, the application verifies the digital signature of the applet, for reconfirmation of its origin. The communication between the background process and the applet is emphasized in figure 4.

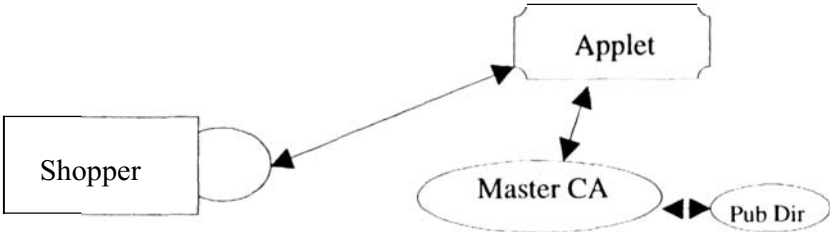

Fig 4.

3.6.4 Summary

This is the last step for securing a client in preparation for secure communication with a possible e-Merchant. This completes the process of establishing the basis of a methodology for secure and correct authentication of communicating parties, as well as for secure transmission of sensitive data over an open network. It is important to note that the process of securing the client, can be performed by anybody willing to adopt the methodology of secure communication as offered by the Master CA. This process does not have to be initiated by an e-Merchant who detects insufficient security on a client's machine; any concerned online shopper can initiate it.

3.7 Communication between shopper and e-Merchant

3.7.1 Download of Merchant applet

Once the securing of the client is complete, there is no need for the above-described procedures to be repeated ever again. The following step can be part of a resumption of a frozen session between a previously unsecured client with the e-Merchant, or as an initial step for submitting sensitive credit information by the client to the Merchant in completing the online transaction. This next step sees a Java applet downloaded from the e-Merchant's web site to the client's machine. The purpose of this applet is to collect sensitive credit information from the client and return it to the Merchant.

3.7.1.1 The Java applet

The Java applet is signed by the Master CA's private key. The applet takes as an external component the Merchant's Digital Certificate. The applet further has security permissions to communicate with the client's background process in the same manner described above as with the communication between the applet used for key pair generation by the Master CA.

3.7.2 Merchant Authentication

Before any sensitive information is entered by the online shopper in the downloaded applet, the IB first verifies the digital signature of the applet. Following this, the applet passes the Merchant's DC to the client's background process. This triggers an authentication procedure by the client's background process:

- Verification of the chain of trust of the Merchant's digital certificate.
- Online check of the Merchant's DC's ID in the issuer of this DC's CRL.
- Final online procedure, involving download of the Merchant's DC from the issuing CA's Public Directory. Then at the client's machine, a verification, of the main attributes of the DC, of the newly downloaded certificate versus the one received from the applet is performed.

In the possibility that at any authentication step yields a negative result, this would indicate an attempt for a security breach by a malicious party and the transaction is discontinued.

3.7.3 Information encryption

Once the authentication process on the client side is complete the shopper is prompted to enter credit information in the downloaded applet. This information is then passed to the client's background process, which includes the shopper's DC and encrypts the whole package with the Merchant's public key, signs it with his Digital Signature private key and passes it back to the applet which in tum transmits it to the online Merchant.

3.7.4 Client Authentication

Once the encrypted data is received, alongside with the Client's Digital Certificate, a chain of trust is established if possible, based on the existing trusted root certificates on the Merchant side. Following this, the certificate's authenticity is checked in the issuing CA's CRL as well as this certificate's validity is checked, by downloading this certificate from the CA's Public Directory and performing a comparison versus the certificate transmitted by the Client. If this authentication process does not run into any problems then credit card information, once decoded is verified using appropriate channels. This completes the transaction and the online shopper is notified of the fact that his/hers transaction has been performed or not.

3.7.5 Summary

The methodology outlined in this section (TTP), represents an effective process for secure authentication of two parties over an open network. The point of trust is a basic CA, which has established chain of trust. The structure of the methodology is such that it does not allow for anonymous communication between two parties, as complete mutual authentication is required before a transaction can be performed. The drawback of the proposed methodology is that it will affect the performance of any secure transaction between hosts and it will require a permanent connection to Cas, for the purpose of CRL verifications. The methodology avoids common pitfalls displayed by implemented technologies now in practice and thus is liable to raise consumer confidence in online trade.

4. EXTENDING THE MODEL

4.1 Weaknesses of proposed model

The above described model serves the purpose of securing a client with the required attributes for him or her to be able to perform a secure and authenticated transaction with another party, equipped with similar attributes, in a semi transparent manner. One of the attributes referred to is a pair of Digital Certificates. These certificates are issued to every client who has applied for them using the described above model or simply on his own initiative applied for them. These two DCs have the purpose of creating a digital identity for an applicant. This digital identity is created and based upon information provided by each applicant. This varies from first name and email address to surname and place of birth. Such information can be easily falsified and thus the digital identity based on it becomes untrustworthy. Examples of such digital identities, based on unverified information are represented by most level one certificates issued by most public CAs, to the general public.

4.2 Creating Trust

It becomes clear from the previous section that verification of user identity becomes vital to the proposed model's functionality. Such authentication of user identity can only be performed by the trusted third party and that is the *Master* CA. User authentication can be performed by a physical verification of the user details, into public records or relative government departments. This is assuming that the *Master* CA is based or has representation in each country, in which it has clients or applicants. Even if this was the case, physical verification of an applicant's identity would take a reasonable amount of time, far beyond what would be considered seamless and transparent process for securing a client, as specified by the proposed model. This would obviously not fit easily or at all in the described scenario of previous sections and would seriously impede the theoretical and practical flow of this methodology. Based on this, the need for an institution, which can easily and quickly verify the identity of an applicant, is required. Considering the fact that an applicant is at the point of purchasing goods or services, before he or she is redirected to the TTP, it must be apparent that this applicant is in the possession of some credit information such as a credit card, which is issued by a reputable financial institution, which are banks in most cases. Such institutions have performed a certain degree of

identification of applicants, based on the fact that all applicants go through a thorough identification process before being issued with appropriate purchasing attributes, such as chequebooks or credit cards. This verification process is already performed at the point of a client wanting to purchase goods or services from and E-Merchant, as he or she is in the possession of at least a credit card.

The placement of trust in an issued digital identity in the form of a certificate, by the TTP, can be done by verifying that the person holding the credit-purchasing attribute is the same as the one to whom this credit attribute was issued. Such verification would confirm the identity of the applicant for a DC and thus place a great trust in the issued certificate. The trust in this certificate will be great because the process for issuing credit purchasing attributes such as credit cards, requires an extensive and thorough identification of the applicant, his or hers financial status as well as previous credit history. The above mentioned verification of credit attributes such as credit card versus the identification details of the applicant for a DC represent a simple mach of these two pieces of information in the financial issuing authority's database. This issuing authority could be represented by a bank but does not necessarily have to be.

4.2.1 Verification details

The specific details required for an applicant to be issued with a high trust certificate, deal with specific purchasing attributes e.g. credit card number, coupled with the card owner's name and a specific secret key. Such a key can be the pin number for this card or some secret code known only by the financial institution and the card owner. This would verify that the card is not merely stolen but it is the possession of its rightful owner. Such supply of information would be necessary for any other purchasing attribute apart from a credit card.

4.2.2 Finalization of authorization

Once all the required information is supplied to the TTP this data is passed to the relevant financial institution or issuing authority of purchasing attributes, such as credit cards, in order for this data to be verified. Once this information is verified, the financial institution can vouch for the identity of the applicant. This will place a very high trust in the resulting Digital Certificate(s). Following this approach, a financial institution such as a bank,

or going higher up the hierarchy a credit card issuing enterprise such as Master Card or Visa, can serve as a authenticating parties in cooperation with a TTP in the process of creation and implementation of the proposed model.

5. CONCLUSION

This paper deals with presenting a new methodology for secure mutual authentication between two communicating parties over an open network. The process described here identifies and outlines clear steps for securing network communications and the data being transmitted in them. It takes a single point of trust in the name of a Certification Authority and with the help of small network based applications and applets constructs authentic way for identifying communicating hosts to one another via the use of asymmetric cryptography and Digital Signatures. The end result represents increased consumer confidence in a possible e-commerce environment, avoidance of current security pitfalls and potential decrease in credit card fraud.

6. LIST OF SOURCES CONSULTED

[SSL 96] The SSL Protocol Version 3.0, **November 18 1996** http://home.netsacape.com/eng/ss13/draft302.txt

[PGP 95] The official PGP User's Guide, P.R. Zimmermann, **1995, MIT Press, USA**

[BPKIC 01] Basic Public-Key Infrastructure Characteristics, Marc Branchaud http://home.xcert.com/-marcnarc//PKYthesis/characteristics **Jan 2001**

[DS 97] Decrypted Secrets Methods and Maxims of Cryptology, F.L. Bauer, **Springer-Verlag Berlin Heidelberg, 1997**

[SON 97] Security on the Net, Eddie Rabinovitch, http://www.cosmoc.org/ci/public/1997/mar/internet_column,html **1997**

[CTNS 00] The Concept of trust in Network Security, Entrust Technologies White Paper, **August 2000,** http://www.entrust.com

[VS 01] Outsourced Authentication Administrator's Guide, VeriSign, **January 2001.** http://www.verisien.com

[SET 97] Secure Electronic Transaction version 1.0, May 31, 1997, Master Card & Visa, http://www.visa.com/nt/ecomm/set/setprot.html

[PWC 98] Electronic Commerce/Internet Survey
http://www.pwcglobal.com/extweb/ncursvres.nsf