

7 CONCLUSIONS AND RECOMMENDATIONS

7.1 Summary of Work Done

The main component of this project was the development of the web based domain registration system for the LK Domain Registry. As a part of this project, the procedure of registering domain names in the registry was formalized and an orderly registration process was developed. This enabled the resolving of problems in registering domains much quickly.

7.1.1 *Evaluating and Enhancing the Security of the Overall System*

As the domains registered under a TLD belong to many different organizations that use them for very crucial processes such as handling their emails, having 24x7 online information, etc, the 100% uptime of the domain name system is essential. It is also important to register domains without much delay, as some organizations need the reservation or registration of domains in a hurry. In doing so, if a part of the registration system or the DNS goes down, it will need to be restored quickly. The project therefore, evaluated the security of the system in much detail and implemented many precautions that were recommended in the CERT reports and that were implemented by other registries.

7.1.2 *Developing the Payment Gateway*

A major portion of time in the project was spent in the development of the payment gateway. It evaluated the structure of the gateway that would suit the needs of the system, by examining the different methods that were currently being used on the Internet. The possibility of using existing infrastructure in Sri Lanka for processing credit cards through banks and point of sale (POS) terminals and emulating such a device through software was the method that was given the most priority in this process. A great deal of

work was done in this regard with the kind assistance of the Hatton National Bank. In parallel, the methods that were available from other international payment gateways were also evaluated. The first payment gateway offered by a local bank, which is the Hong-Kong and Shanghai Bank's payment gateway was also evaluated as a solution to the payment gateway requirement of the LKNIC.

7.1.3 Developing the Certification Authority

On the part of developing the CA, the main part was the installation of the Open CA software locally and evaluating it. This was a major achievement as the installation versions available at that time were all beta releases and had many problems in the installations. The author was able to contribute to the development of the Open CA project by actively producing bug reports to the Open CA development mailing list. The locally installed CA was able to generate, sign and issue certificates to the Netscape browser only, as the issuing of certificates to other browsers was not available. The project also evaluated several other options of having a major CA being represented in Sri Lanka by having a registration authority by LKNIC. The registration authority of VeriSign was the main candidate for this.



University of Moratuwa, Sri Lanka.
Electronic Theses & Dissertations
www.lib.mrt.ac.lk

7.1.4 Developing the Web-Based Registration System

The web based registration system was the main achievement of the project. Because of the new interface, and the facilities available through it, it is now possible for someone to register a domain even within one day. Since the system is now a distributed system, the administrators can access and register domain names even if they are not in the country. Because of the special features like multiple domain registrations by copying from existing records, it has been possible to register requests of even 50-60 domains from the same organization with ease. There were several occasions where this feature was used in the early days of the system. The generation of resource records automatically and the online verifications of the data entered has resulted in reducing the errors that occur in registering domain names.

Because of all of these reasons, it has been possible to cater for the increased demand in registering domain names. The graph in Figure 14 shows the number of domain registrations for each month from January 1998. This shows a significant increase in the domain registrations including some months that have registrations exceeding 100 domains per month.

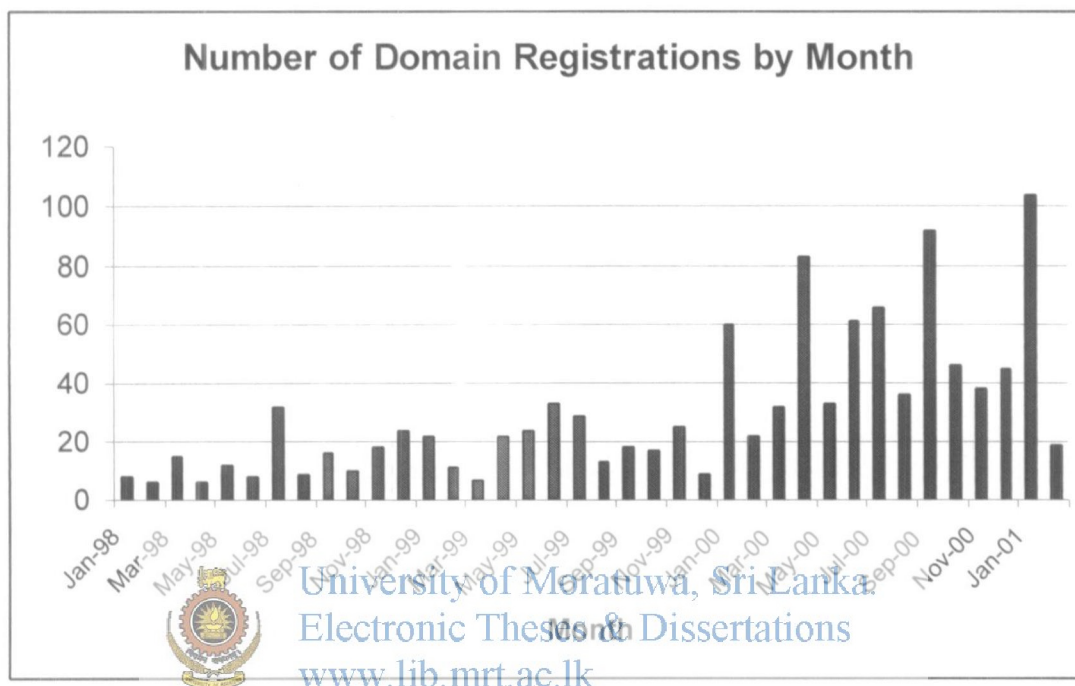


Figure 14 : Number of domain registrations per month

7.2 Experiences

The main and unforgettable experience from the project to the author is the work done as the Hostmaster for the LKNIC. This brought about many opportunities to him. The main opportunity was the in-depth learning an experience of handling an actual name server. He gained a great deal of experiences in this area by helping other parties to get their name server problems solved. The experiences gained helped in figuring out the common problems quickly and handling them without much delay.

The work as a member of the Internet committee of the CINTEC, gave him the opportunity of being a participant in making national policy decisions in the field of IT.

The pleasure of working with some of the top-level people in the industry and the wealth of knowledge gained from them is immense.

Visits to the various international conferences and meetings as a part of this work helped him gain not only knowledge of what other NICs were doing in this area, but also knowledge of what developments they had in the IT field. He was able to get firsthand information about ongoing research in the fields such as multilingual domain names, DNSSec, IPV6, etc.

The work with the HNB enabled him to get some inside information about the internal operations of a bank. It also provided knowledge in what developments were there in the banking sector and the things to expect in the future.

7.3 Common Problems Encountered

Finding out information for the relevant technologies was the most common problem encountered. Since this field was new and rapidly developing, there were not many books available locally on the topics. The area of domain registration is also done by a handful of organizations and hence there are only a few places to obtain additional information.

Many problems were encountered during the implementation of the payment gateway as this involved dealing with areas that have high security and risks of entire organizations going down in business. This was the case with Hatton National Bank, where they were reluctant in certain cases to go ahead with tests on the live system. In other cases, the technical staff refused to co-operate until they were given the OK from the top-level management.

The information about the different protocols that are used on POS terminals were the most difficult to figure out as even the technical staff at the company handling the installations of the devices locally did not have any clue as to what they were. Most of these were guessed by going through the different brochures and manuals that were found from the web sites of the POS terminal manufacturing companies.

Contacting the different payment gateway service providing companies was a major obstacle mainly because they requested calling international phone numbers and the time differences involved were also inconvenient. In some of the cases the phone numbers provided were also found to be incorrect. Some of them were reluctant in responding to questions before any payments were made to them.

The implementation of security on the system was a problem as not all recommended precautions could be implemented. This was mainly due to the lack of resources. Since the provision of resources requires the approval from several parties, it was compelled to share resources with other systems to get the system operational. But when the resources are available, these should be utilized to obtain the highest possible security levels.

In the processing of the domain names, the problem of deciding on generic names was a major problem. Since the term generic name is a very open classification, it was difficult at times even for the panel to decide on whether to approve the domains or not. A refinement on this policy was required and many parties who requested generic names also requested a more open domain policy. With this in view, several second level domains were proposed to the Internet committee. One of these domain names, the web.lk domain will soon be made available.

7.4 Future Enhancements

The part on making the online payment gateway operational still remains, as the costs involved were too high. But the main functionality required to process online domain requests have already been implemented. The only section pending development is the development of the payment acceptance. This part will take away many of the complications encountered when registering domain names by foreign parties.

Currently there has not been any developments done in implementing a renewal process for the domains. This part is partially facilitated by the existing system, but as a proper renewal procedure was not finalized, development of this module was not done. Once a

proper renewal procedure has been defined, it can be implemented easily as most of the functionality is already available in the coding of existing modules.

The introductions of further second level domains under the .lk domain structure and the introductions of domain registration authorities are essential for the development of the LKNIC. This has already begun with the introduction of the web.lk second level domain. With the developments that have been done for the implementation, several improvements were done to the system. They were designed to facilitate the introduction of future second level domains and registration authorities without much difficulty. These introductions will require a further level of administration.

The new second level domains incorporate more strict formats to the resource records, which enable the complete generation of the zone files automatically. This has been possible because of the experiences that were obtained in implementing the current system.

Once these functionality are finalized, it would be possible to compare it with most of the leading domain registration systems in the world. It would also be able to link up with such systems to facilitate the registration of .lk domains through external systems.



University of Moratuwa, Sri Lanka.

Electronic Theses & Dissertations

www.lk.mru.ac.lk

APPENDICES



University of Moratuwa, Sri Lanka.
Electronic Theses & Dissertations
www.lib.mrt.ac.lk

APPENDIX A - PUBLIC KEY INFRASTRUCTURE

Electronic transactions are now becoming common in the day to day life of people. It is a very common thing today for you to browse through the web, find a suitable product, and order it online using your credit card as the method of payment. But how safe is this common transaction? Is this same method of transaction safe to use with a transaction of millions of dollars?

Introduction to Cryptography

The definition of cryptography is using encryption to conceal text or messages. Cryptology is the term that defines the study of encryption and decryption and for the person trying to break into the message, his job is defined as cryptanalysis. [17, 18] Cryptography depends very highly on mathematical formulas that are believed to be very difficult to break into using commonly available resources. A breakable cryptographic technique is one that can be broken into given sufficient time and data. Very good crypto techniques can be broken into only using very powerful super computers for a very long period of time, by which time the information that is retrieved will be worthless due to the lapse of time.

Data that can be read and understood without any special measures is called *plaintext* or *cleartext*. The method of disguising plaintext in such a way as to hide its substance is called *encryption*. Encrypting plaintext results in unreadable gibberish called *ciphertext*. You use encryption to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting ciphertext to its original plaintext is called *decryption*.

There are two types of cryptography that are widely used on the Internet.

Symmetric Cryptography

Symmetric cryptography uses same key for both encryption and decryption. Because of this, if the key is lost from one party, the other party is also vulnerable for attacks. The key distribution in these systems is also a problem because if the key becomes known by a third party, a new key needs to be distributed to all the users if a secure message is to be sent again. The key distribution requires a secure channel if the security is to be ensured.

The main advantage of symmetric cryptography protocols is that they have very fast algorithms and also hardware level implementations of the protocols such as DES. Therefore, most of the asymmetric cryptographic systems use symmetric cryptography

for exchange of the bulk of data after exchanging a session key using asymmetric cryptography.

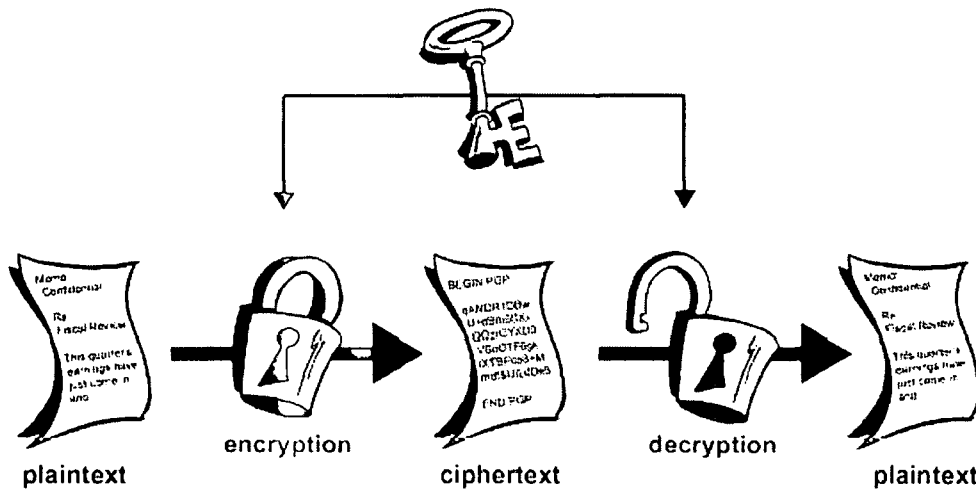


Figure 15: Symmetric Encryption

The process of encryption and decryption are illustrated in Figure 15. It clearly shows that the same key is being used for both the encryption and the decryption.

Asymmetric Cryptography University of Moratuwa, Sri Lanka.
Electronic Theses & Dissertations

To overcome the problems encountered in symmetric encryption, asymmetric encryption methods were introduced. Asymmetric cryptography has added advantages over symmetric encryption mechanisms as it can also provide additional services like authentication, non-repudiation and integrity.

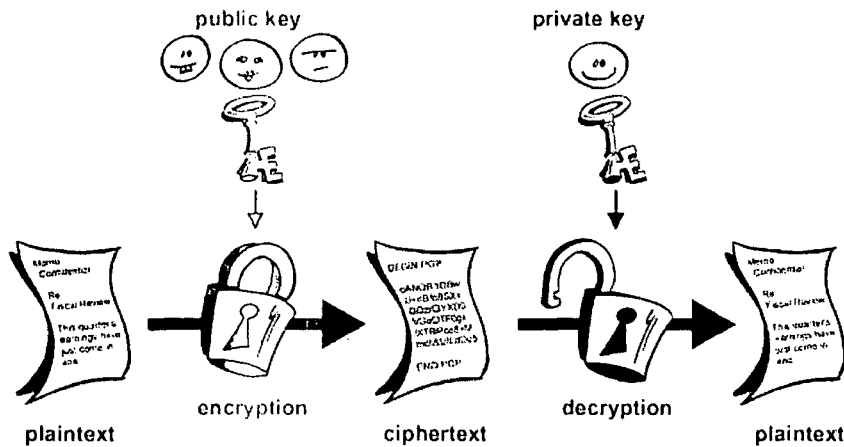


Figure 16: Asymmetric Encryption

Asymmetric encryption as illustrated in Figure 16, uses different keys for encryption and decryption. The public key as its name indicates is made available publicly so that any party that wants to do a secure communication with the party interested can obtain their public key and encrypt the data. The private key on the other hand is the secret that will only be available with one party. The secrecy of the private key is essential for the implementation of the additional services like authentication, non-repudiation and integrity. If the private key is compromised, the use of the corresponding public key is made useless for encryption purposes.

Public Key Infrastructure

The major challenge in asymmetric encryption methods is the distribution of the public keys corresponding to the different entities and guaranteeing that the correct identity is associated with the public key. To address these issues, public key infrastructures have evolved which again utilize encryption mechanisms to ensure their correctness.

Trusted third parties have evolved to address the issue of distribution of public keys with a higher level of authenticity. These organizations are called Certification Authorities (CAs). These organizations use digital data elements called certificates that encapsulate the public key of the entity involved and include a digital signature to it.

Digital Certificates

A certificate is a binding between an entity's public key and one or more attributes relating to this identity. The entity can be a person, a hardware device or a software process. The certificate provides assurance that the public key belongs to the identified entity and that the entity possesses the corresponding private key.

A digital certificate has in general terms the same purpose as an identification card such as a driver's licence or a passport. A driver's licence or passport binds a photograph of the subject with a name, address and other information. This binding is valid only if the identity was issued by a trusted party of the entity that will use the license or passport to authenticate the subject. If the issuing of such identities is not properly regulated, then others will not trust the binding between the picture and the information.

If the identification document can be easily manipulated by another party to alter the information carried in it, again the trust on that identity document will be lost. Similarly, the digital certificates too need some form of preventing tampering of the information. This is achieved by a digital signature on the certificate which is basically an encryption of a message digest of the information in the certificate using the public key of the certification authority.

Certification Authority

A certification authority is a trusted third party that issues digital certificates to entities. The trust of these third parties could be established by the distribution of their public keys

via some trusted mechanism. The trust on these parties should also be built on the assurance that they verify the validity of the information that are bound with the public key of the entity. If this trust is broken, the certificates issued by that CA would soon be untrusted and discarded by users.

The public key of the CA is usually distributed with the browsers that use the certificates. It could also be incorporated into a browser by downloading or copying it from a known trusted source.

X.509

X.509 is the standard defined by the International Telecommunication Union-Telecommunication Standardization Sector (ITU-T) and ISO/International Electrotechnical Commission (IEC) for digital certificates. The first version of this was published in 1988 as a part of the X.500 Directory recommendation. The X.509 version 1 (v1) was later extended in 1993 to incorporate two new fields to support directory access control, which resulted in producing version 2 (v2). In 1993, the attempt of implementing Privacy Enhanced Email (PEM) revealed that both v1 and v2 of X.509 were having deficiencies. The revision of v2 at that time implemented a few other fields into the format yielding version 3 (v3) in June 1996. [19]

The structure of the X.509 v3 certificate is illustrated in Figure 17.

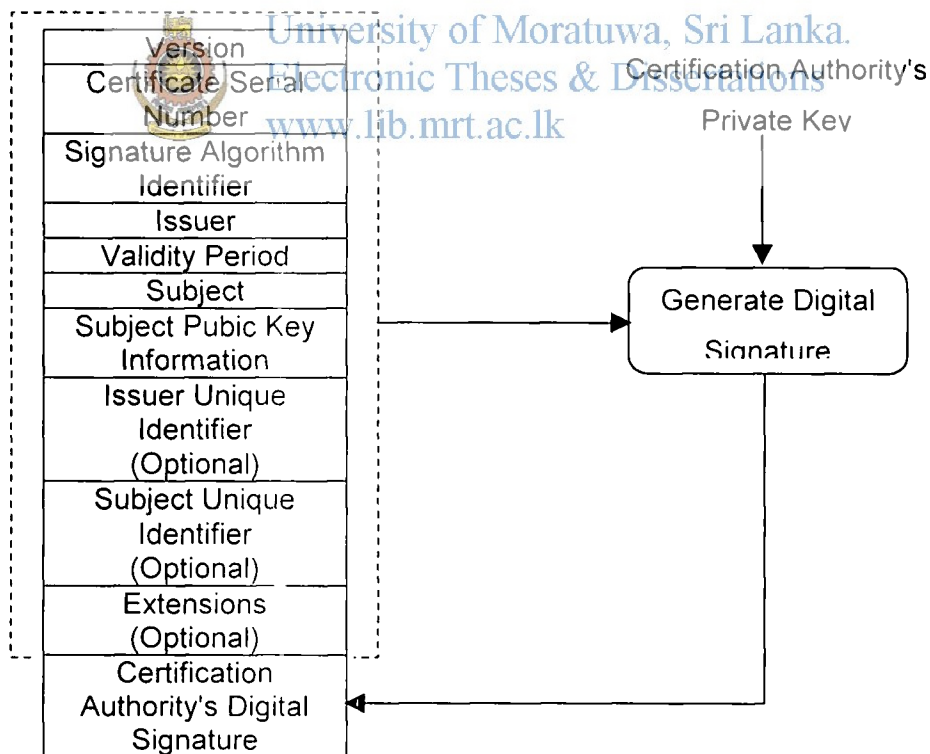


Figure 17: X.509 v3 Certificate Format

The information carried in each of the fields are as follows:

Version: The version number of the encoded certificate.

Certificate Serial Number: An integer assigned by the CA, which is a unique ID that can be used to trace the certificate.

Signature Algorithm Identifier: This field identifies the algorithm, such as RSA or DSA, used by a CA to digitally sign a certificate.

Issuer Name: The name of the CA that signed and issued the certificate.

Validity period: Time interval during which the certificate remains valid and the CA is obliged to maintain records of the certificate during this period. The field carries a start date and an end date.

Subject name: The identity of the entity whose public key is certified in the certificate.

Subject Public Key Information: Contains the public key material (public key and parameters) and the identifier of the algorithm with which the key is used.

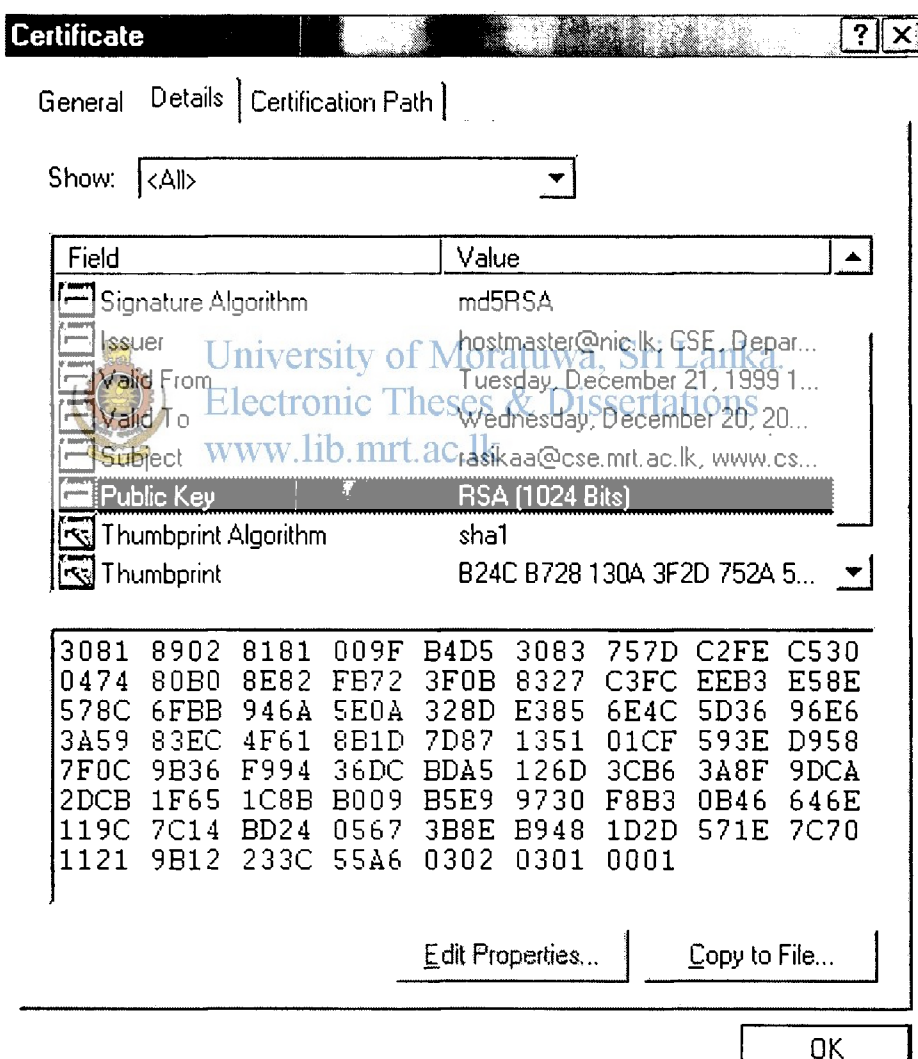


Figure 18: A Certificate



Issuer Unique Identifier: An optional field to allow the re-use of issuer names over time.

Subject Unique Identifier: An optional field to allow the re-use of subject names over time.

Extensions: Provides a way to associate additional information for subjects, public keys, managing the certification hierarchy and managing certificate revocation list distribution.

A certificate as it is shown on a browser is illustrated in Figure 18.

Certificate Hierarchy

The certificates that are issued carry a signature of the issuer CA. This is basically some encoded data that is encrypted using the CA's private key. In order to verify the integrity of the certificate, the receiving party must re-encode the data using the same algorithm that was used for the generation of the signature and verify this with the decrypted signature. In order to decrypt the signature, it needs to obtain the public key of the CA. The public key of the CA is usually embedded in another digital certificate. Who will be the issuer of this certificate?

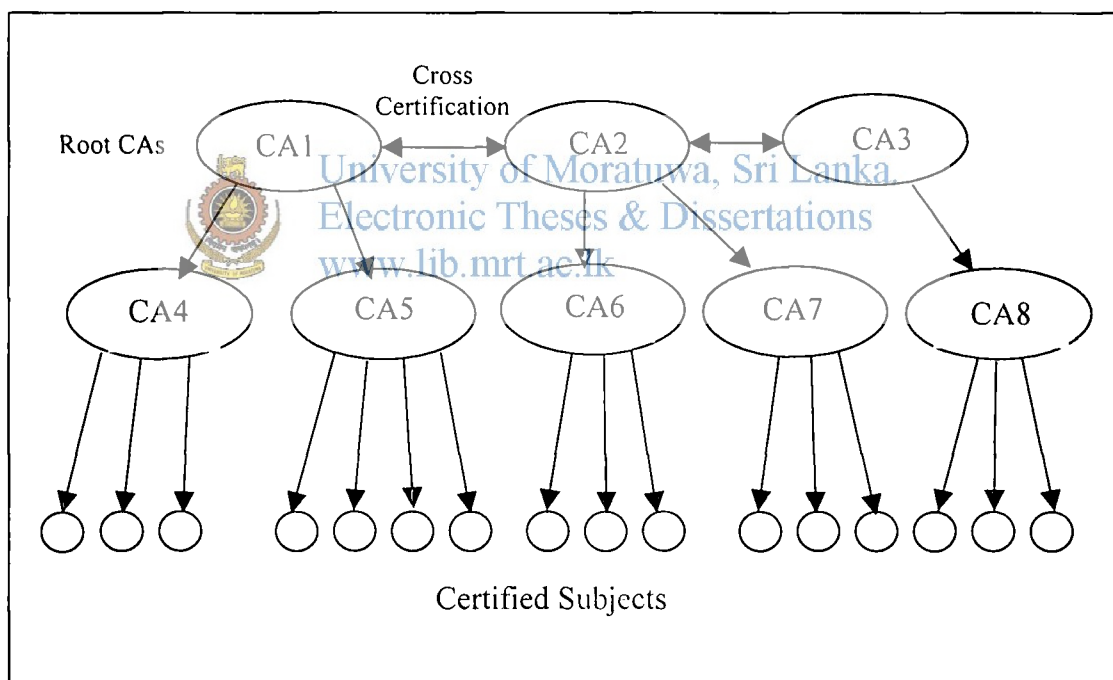


Figure 19: Certificate Hierarchy

A CA may self sign its own certificate and distribute it in some secure manner to the public or several CAs at the top may cross certify their certificates while one or more of them will have the certificates distributed in the former manner. Lower level CAs could also be certified by higher level CAs which are usually called Root CAs. This hierarchy of certification can lead to the ultimate verification of all certificates on the Internet as illustrated in Figure 19.

Certificate Issuing

The issuing of certificates by a CA may be handled in different mechanisms. The usual practice is for the applicant entity to create a key pair using some software such as a Java applet running on a web browser and send the public key along with the relevant information as a request to the CA. If the CA is very large, it may have regional offices or distributed agents called Registration Authorities (RAs) to handle the requests and authentication.

The request is authenticated by means of checking the identity of the entity by checking legal documents, the ability to receive emails on a specific email address, etc. The authenticated request is then converted to a digital certificate that is given a validity period and signed by the CA. The signed certificate can then be issued to the applicant via the web, diskettes or on a smart card depending on the requirements of the applicant.

Certificate Distribution

A CA may provide a certificate distribution service for a certificate-using system to access and obtain a subscriber's certificate. A person may, for example, use this service to look up another person's certificate, download the certificate into an email application and send a secure email to that person. The distribution can be done in several ways. The most popular methods are directory servers and email.

X.500, is one of the methods of distributing certificates in a directory. X.500 could be used to distribute other forms of information too. But the complexity of implementing X.500 directory servers has hampered their widespread use in the Internet community. LightWeight Directory Access Protocol (LDAP) is a scaled down version of X.500 and is currently one of the most popular directory protocols used for certificate distribution. Using LDAP it is possible to implement client side applications that can access certificates much easily.

On the other hand, a CA may use ordinary or secure emails to send the certificate of a client to a requesting party directly.

Certificate Revocation

Once a certificate is signed and issued, it has a binding on the public key that is associated with it. This public key has a corresponding private key that the subject is supposed to be keeping secret. But secrets may be compromised and the private key may become public. At this point the use of that private key for secure communication is of no avail. The subject should make arrangements to inform the CA about the compromising and use a new key pair instead.

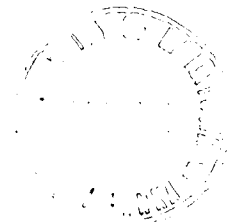
A new key pair means a new public key too. As a new public key cannot be used with the same certificate that was used earlier, a new certificate needs to be issued by the CA. At this point, there is the old certificate, which could have local copies of it being used by

parties who obtained it earlier for communication with the subject. If they are to know that the certificate is no longer valid, it should be informed. The discovery by the CA that the party that has obtained the certificate is not the real party that it claims to be also requires the cancellation of the certificate. This requires some mechanism for the revocation of the certificates.

CAs use a mechanism called Certificate Revocation Lists (CRL) to handle this problem. The CRL is available in a standard format that is again defined under X.509. The client using the certificate could check the CRL of the issuer CA to check if the certificate that it has received is valid. If the certificate is revoked, the user can be informed of the situation and security problems could be overcome.



University of Moratuwa, Sri Lanka.
Electronic Theses & Dissertations
www.lib.mrt.ac.lk



APPENDIX B - ELECTRONIC PAYMENTS FOR E-COMMERCE

Payments have been used throughout the history of mankind as remuneration for the supplying of products or services. The payment mechanisms evolved from the simple barter systems, through the use of symbolic instruments as money and then to the use of documents with certification such as cheques and money orders. The electronic era introduced further mechanisms of payment by introducing credit and debit cards whose validity and credit limits could be checked electronically thereby improving their effectiveness.

History of Electronic Payments

The evolution of electronic payments was greatly facilitated by the fact that the cost per transaction of electronic means is far below those of paper based ones. The reduction of the cost has been mainly due to the use of the Internet as the main carrier of information over proprietary private communication channels that were used in the early stages.

During the initial stages of electronic payments, the security of the information was very important and banks and other financial institutions had built their own private networks to communicate the information. They used proprietary protocols, which were kept very secret. The main types of communication that were carried over these lines were transfers from one account to another, within the same bank network, the checking of account balances and updating of account transactions that were done, out of the normal operations branch etc. Credit and debit card systems were introduced by many financial institutions that were facilitated by these networks.

The use of proprietary protocols by different institutions restricted and discouraged the inter-institute transactions limiting the types of operations. Credit and debit cards that were used in one institution could not be used in another institution, as the systems were not integrated. As the demand for more and more integration and globalization of services increased, the financial institutions were compelled to inter operate. This led to banking networks such as SWIFT (Secure Wire International Funds Transfer). These networks facilitated the transfer of funds from one bank to another bank electronically. The actual transfer of funds was done at the end of a period by means of a net transfer of physical funds limiting the physical movement of money.

International credit card systems spread their wings all over the world providing the facility for cardholders to make payments through them anywhere in the world. The card payment companies widened their networks by utilizing the new and emerging

technologies of cryptography, which enabled them to use cheap and insecure channels such as the Internet for the transfer of sensitive information, securely. The widened coverage of card systems lead to the use of credit cards as a popular means of making payments at remote locations.

Credit cards became a method of making payments for orders that were made by post. The cardholders used the credit card number and signed in the form authenticating the merchant to make the funds transfer. The merchants could check the validity of the card through a terminal at his premises before providing the goods or services. The system then widened its scope with the innovation of making orders over the phone. The requirement of a signed authentication from the cardholder was slackened and the card number plus some additional information such as the date of expiry of the card, the name and address of the card holder, etc. were used by the merchants to verify whether the person making the order actually possessed the card.

With the wider popularity of advertising products and services over the Internet, it was soon discovered that the method of mail orders or phone orders could be easily extended to the Internet. Initially the card information was directly accepted over the Internet and the merchant did manual verification of the card. Software developers soon developed software that could directly get the card information, verify the card and make the payment authenticated in real time thereby eliminating long delays of processing.

However, there were many problems with these methods. The transfer of the card information over insecure channels like the Internet made the card information vulnerable to be picked by hackers and used again on the Internet to make spoofed payments. More secure methods of sending the card information such as the use of SSL and other encryption methods and online use of address verification etc. were introduced to overcome these problems.

Current Methods

Today, the credit cards and debit cards are still the most popular mechanism of making electronic payments. Newer methods such as electronic cheques and e-cash have evolved to make payments over the Internet much easier. We will look at some of these methods in detail.

There are two main types of electronic payments used for e-commerce in the world. They are:

Stored account payment schemes

Stored value payment schemes. [20]

Stored Account Payment Schemes

Stored account payment schemes designed for e-commerce simply represent new ways of accessing traditional banking services to shift funds electronically over the Internet. In this type of payments, the actual monetary value of the of the transaction never leaves the

bank vaults, but is, instead accounted for, at some time in the future through clearing houses and settlement systems. High accountability and traceability are hallmarks of stored account payment schemes. This has led to concerns about privacy of payments made. With full traceability of commercial transactions, a history of purchases can be compiled to establish personal profiles of spending habits for anyone. These profiles, in turn can be used for targeted advertising or perhaps for unlawful pursuits by threatening to disclose previous spending patterns.

The main disadvantage of stored account payments schemes over the privacy problem is that it needs online verification. Real-time online verification can significantly increase the cost of the transaction as well as introduce delay in the approval of transactions.

One of the most widely popularized and recommended schemes for stored account payment schemes is the Secure Electronic Transaction (SET) protocol, which was jointly developed by Visa and MasterCard, the two giants in the credit and debit card arena. Other methods that were in use are First Virtual's Internet Payment System [21] and CyberCash's Secure Internet Payment System [22].

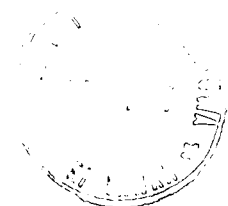
Secure Electronic Transaction (SET)

As mentioned earlier, Visa and MasterCard jointly developed this protocol with several other computer and Internet giants. SET is fast becoming an accepted standard for processing credit card based transactions over insecure communication channels such as the Internet. SET uses cryptography to provide confidentiality and security, ensure payment integrity, and authenticate both the merchant and the cardholder. This security means that merchants are protected from purchases with an unauthorized payment card and can deny purchases to cardholders, banks are protected from unauthorized purchases, and cardholders are protected from merchant imposters or theft of their payment card numbers. [23, 24]The SET protocol is illustrated in Figure 20.

The steps involved are:

Certificate retrieval: Before a transaction can start, each of the parties involved must obtain certificates. Certificates assist in the authentication process. The gateway (1), the merchant (2) and the cardholder (3) obtain their own certificates from the Certification Authority (CA).

Purchase: The steps encompass what is normally thought of as the "heart" of the transaction, even though other steps are involved in the purchase transaction as a whole. First, the cardholder shops at the merchant's (online) shopping mall and decides what goods or services that he wants to buy (4). The merchant then sends the cardholder the certificates that are required in the purchase transaction (5). The cardholder sends a request to purchase the items that he has selected. This message contains information about the cardholder's order and the cardholder's payment information such as the card information. The merchant gets the order information and sends the cardholder's payment card information to the payment gateway (6). **The merchant never gets the cardholder's payment card information.**



The merchant and payment gateway then send authorization information. This consists of the merchant sending the payment gateway information such as the cardholder's payment card information and the amount of the transaction and the gateway authorizes the payment (7). No money transfer has been made at this stage. The merchant then sends a message to the cardholder finalizing the transaction. This is what cardholder sees as the end of the transaction (8). In the optional step (9) allows the merchant to change or eliminate money authorized in step (7).

Capture: The capture phase handles capturing of money that has been authorized in step (7). It also handles reversal of captured money if needed. Money authorized is usually captured by the merchant in some predetermined regular time frame, such as at the end of every day. For this the merchant and the payment gateway share capture information. (10). If an error occurred capturing cardholder's funds, messaging between the merchant and the gateway takes place in order to reverse the capture (11). This step is optional and only happens if a capture error has occurred.

Credit: Sometimes a merchant needs to credit a cardholder's account. The merchant and payment gateway exchange messages in order to credit a cardholder's account (12). If a credit has been granted by mistake, the merchant and payment gateway can exchange messages in order to reverse the granted credit (13). [23]

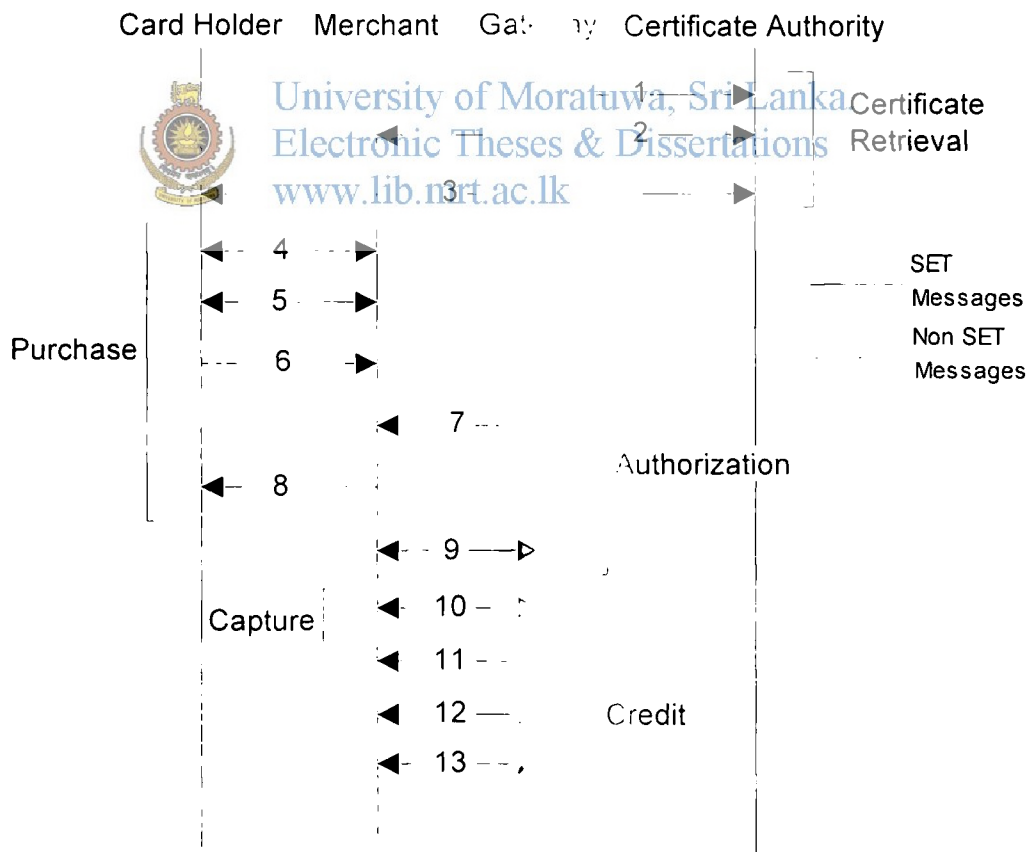


Figure 20: Steps in the SET Protocol

More details of the SET protocol can be found from [23] and [24].

Stored Value Payment Schemes

Stored value schemes in contrast attempt to replace cash with its electronic equivalent, e-cash, by transferring a unit of money between two parties. The transfer of value is instantaneous because it does not require approval from a bank, and banking accounts are neither credited nor debited during the transaction. The security risks associated with stored value systems are much higher than with stored-account schemes because of the absence of control and auditing and the possibility of undetectable counterfeiting.

The security concerns of using stored-value schemes constitute one reason. E-cash is typically used for small value transactions such as pay-per use schemes for online publications. Another more motivating factor is the size of the currently untapped small value transaction market. A lot of small value transactions can add up to whole lot of money.

Some of the stored value schemes that are in use are Millicent[25], which was originally designed by Digital and now owned by Compaq, DigiCash [26], CyberCoin [27] and Mondex[28].



University of Moratuwa, Sri Lanka.
Electronic Theses & Dissertations
www.lib.mrt.ac.lk



APPENDIX C - WEB BASED INTERFACES

Normal computer software will require a certain operating system and other resources to run on. If they are to be able to accessible at different locations, the locations too will need certain parts of the software to be installed at that location. The main advantage that web based interfaces have is that they use the web browser as the interface to the software and usually the application will be running on a web server that would be available on the Internet. So, the application can be accessed using virtually any machine on the Internet that has a web browser. The processing is all done at the server end and this eliminates the requirement of special hardware or software, at the machine accessing the application.

Common Gateway Interface

The Common Gateway Interface (CGI) is the protocol by which programs interact with Web servers. The versatility of CGI gives programmers the opportunity to write gateway programs in almost any language, although there are many trade-offs associated with different languages. Without this ability, making interactive Web pages would be difficult at best, requiring modifications to the server and putting interactivity out of the reach of most programmers, who are not also site administrators.

CGI scripts usually reside in a special directory named /cgi-bin in the web server. This directory has the additional feature of letting the programs in that directory, to be executable in the web server. When a web request is made to access one of the programs on the cgi-bin directory, the specific program is executed with whatever data, that was passed over with the request, as being parameters. This special ability of passing parameters is the main gateway for a CGI programmer to obtain interactivity.

The parameters that are passed could be from a web-based form, the web browser itself or environment variables in the web server itself. These parameters can be utilized in an unlimited combination limited only to the imagination of the programmer to build web based applications ranging from simple guest books to shopping carts to complex secure access banking and financial systems.

Web Based Database Applications

Today it is very common to have database applications with web based interfaces. Some leading database vendors provide modules that even provide the database administration over web based interfaces. The addition of a database back-end to a CGI program further extends the unlimited options of a CGI programmer.

Databases are capable of storing and retrieving large amounts of data in an orderly manner very efficiently. This feature is very important when designing web based applications as the performance of the scripts is very vital on the Internet world when catering for an unknown number of customers. The number of clients that might connect to a given web server at a given time could even be in the range of millions. In these situations the utilization of the available resources effectively is very vital.

Databases are specifically designed to perform the data manipulation tasks effectively utilizing the minimum of resources. Instead of re-inventing the wheel, the CGI programmer can utilize these features effectively by interfacing the CGI programs with the database through the different interfaces that are provided with the different databases.

Secure Servers

In web based applications, there could be situations that will require the transfer of sensitive information from the browser to the web server. If this information goes to an unwanted party, it could lead to severe damage to both the client party as well as the party providing the server. In order to prevent such mishaps, the data that is sent can be encrypted, so that even if a third party gets hold of the data, it would be difficult for them to read the data easily.

Web servers that can handle the secure protocols or other secure mechanisms are called secure servers. These servers are usually extensions of general web servers with modules for the encryption mechanisms. A secure server will usually use some asymmetric encryption mechanism with a combination of a symmetric encryption mechanism to provide the security. It would also be able to authenticate itself with the client and if required for higher security, authenticate the client too, using digital certificates.

Secure Sockets Layer (SSL)

Different implementations of such encryption mechanisms have been used in the Internet.

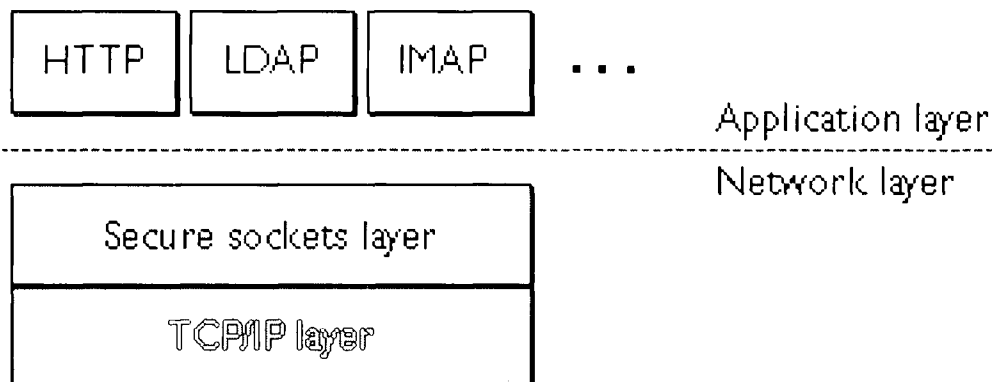


Figure 21: Structure of SSL



The most common and widely used method for such transactions is the use of Secure Sockets Layer (SSL) that was developed by Netscape.

SSL is a protocol that can be used for many other functions other than for web browsers. It is actually a protocol layer sitting in between the application layer protocols and the network layer protocols as illustrated in Figure 21. This layering enables it to be very versatile and independent. [29]

SSL provides solutions to the following fundamental concerns of a secure communication.

SSL server authentication allows a user to confirm a server's identity. SSL-enabled client software can use standard techniques of public-key cryptography to check that a server's certificate and public ID are valid and have been issued by a CA listed in the client's list of trusted CAs. This confirmation might be important if the user, for example, is sending a credit card number over the network and wants to check the receiving server's identity.

SSL client authentication allows a server to confirm a user's identity. Using the same techniques as those used for server authentication, SSL-enabled server software can check that a client's certificate and public ID are valid and have been issued by a CA listed in the server's list of trusted CAs. This confirmation might be important if the server, for example, is a bank sending confidential financial information to a customer and wants to check the recipient's identity.

An encrypted SSL connection requires all information sent between a client and a server to be encrypted by the sending software and decrypted by the receiving software, thus providing a high degree of confidentiality. Confidentiality is important for both parties to any private transaction. In addition, all data sent over an encrypted SSL connection is protected with a mechanism for detecting tampering.

The SSL Handshake

The SSL protocol uses a combination of asymmetric and symmetric key encryption. An SSL session always begins with an exchange of messages called the SSL handshake. The handshake allows the server to authenticate itself to the client using asymmetric key techniques, then allows the client and the server to cooperate in the creation of symmetric keys used for rapid encryption, decryption, and tamper detection during the session that follows. Optionally, the handshake also allows the client to authenticate itself to the server. The steps involved in a SSL handshake can be summarized as follows.

The client sends the server the client's SSL parameters such as version, cipher settings, randomly generated data, and other information.

The server sends the client the SSL parameters such as version, cipher settings, randomly generated data, and other information. The server also sends its own certificate and, if the

client is requesting a server resource that requires client authentication, requests the client's certificate.

The client uses some of the information sent by the server to authenticate the server. If the server cannot be authenticated, the user is warned of the problem and informed that an encrypted and authenticated connection cannot be established and proceeds on further steps depending on the users discrete.

Using all data generated in the handshake so far, the client creates the premaster secret for the session, encrypts it with the server's public key, and sends the encrypted premaster secret to the server.

If the server has requested client authentication, the client also signs another piece of data that is unique to this handshake and known by both the client and server. In this case the client sends both the signed data and the client's own certificate to the server along with the encrypted premaster secret.

If the server has requested client authentication, the server attempts to authenticate the client. If the client cannot be authenticated, the session is terminated. If the client can be successfully authenticated, the server uses its private key to decrypt the premaster secret, then performs a series of steps (which the client also performs, starting from the same premaster secret) to generate the master secret.

Both the client and the server use the master secret to generate the session keys, which are symmetric keys used to encrypt and decrypt information exchanged during the SSL session and to verify its integrity

The client sends a message to the server informing it that future messages from the client will be encrypted with the session key. It then sends a separate (encrypted) message

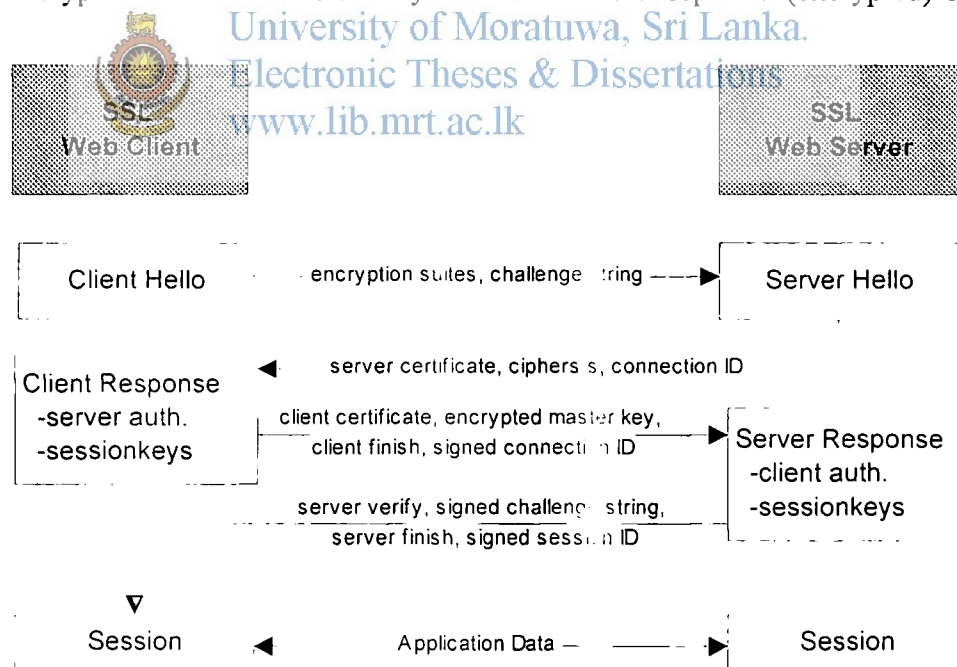


Figure 22: SSL Session Setup

indicating that the client portion of the handshake is finished.

The server sends a message to the client informing it that future messages from the server will be encrypted with the session key. It then sends a separate (encrypted) message indicating that the server portion of the handshake is finished.

The SSL handshake is now complete, and the SSL session has begun. The client and the server use the session keys to encrypt and decrypt the data they send to each other and to validate its integrity.

This process is illustrated in Figure 22. Detailed descriptions of the server and client authentication mechanisms are available in Netscape's introduction to SSL document [29], in chapter 7 of Digital Certificates [19] and in Chapter 3 of E-Commerce Security [20]. The SSL version 3 standards are available at Netscape's web site [30].



University of Moratuwa, Sri Lanka.
Electronic Theses & Dissertations
www.lib.mrt.ac.lk



APPENDIX C - STRUCTURE OF THE TABLES

Domains Table

Field	Type	Null	Key	Default	Extra
d_domain	varchar(50)		PRI		
d_name	varchar(100)				
d_org_desc	varchar(100)	YES		NULL	
d_reason_for_selecting	varchar(100)	YES		NULL	
d_admincont	varchar(100)	YES		NULL	
d_aaddr	varchar(200)	YES		NULL	
d_atel	varchar(50)	YES		NULL	
d_afax	varchar(25)	YES		NULL	
d_aemail	varchar(50)	YES		NULL	
d_techcont	varchar(100)	YES		NULL	
d_taddr	varchar(200)	YES		NULL	
d_ttel	varchar(50)	YES		NULL	
d_tfax	varchar(25)	YES		NULL	
d_temail	varchar(50)	YES		NULL	
d_billcont	varchar(100)	YES		NULL	
d_baddr	varchar(200)	YES		NULL	
d_btel	varchar(50)	YES		NULL	
d_bfax	varchar(25)	YES		NULL	
d_bemail	varchar(50)	YES		NULL	
d_ns1	varchar(25)	YES		NULL	
d_ns2	varchar(25)	YES		NULL	
d_ns3	varchar(25)	YES		NULL	
d_nsip1	varchar(15)	YES		NULL	
d_nsip2	varchar(15)	YES		NULL	
d_nsip3	varchar(15)	YES		NULL	
d_mx1	varchar(25)	YES		NULL	
d_mx2	varchar(25)	YES		NULL	
d_mx3	varchar(25)	YES		NULL	
d_mxip1	varchar(15)	YES		NULL	
d_mxip2	varchar(15)	YES		NULL	
d_mxip3	varchar(15)	YES		NULL	
d_mxpr1	int(11)	YES		NULL	
d_mxpr2	int(11)	YES		NULL	
d_mxpr3	int(11)	YES		NULL	
d_isp	varchar(10)	YES		NULL	
d_effdate	date	YES		NULL	
d_comments	text	YES		NULL	
d_orig_date	date	YES		NULL	
d_mod_date	date	YES		NULL	
d_last_rev	int(11)	YES		NULL	



University of Moratuwa Sri Lanka
Electronic Theses & Dissertations
www.theses.mrt.ac.lk

Requests Table

Field	Type	Null	Key	Default	Extra
q_domain	varchar(50)		PRI		
q_name	varchar(100)				
q_org_desc	varchar(100)	YES		NULL	
q_reason_for_selecting	varchar(100)	YES		NULL	
q_admincont	varchar(100)	YES		NULL	
q_aaddr	varchar(200)	YES		NULL	
q_atel	varchar(50)	YES		NULL	
q_afax	varchar(25)	YES		NULL	
q_aemail	varchar(50)	YES		NULL	
q_techcont	varchar(100)	YES		NULL	
q_taddr	varchar(200)	YES		NULL	
q_ttel	varchar(50)	YES		NULL	
q_tfax	varchar(25)	YES		NULL	
q_temail	varchar(50)	YES		NULL	
q_billcont	varchar(100)	YES		NULL	
q_baddr	varchar(200)	YES		NULL	
q_btel	varchar(50)	YES		NULL	
q_bfax	varchar(25)	YES		NULL	
q_bemail	varchar(50)	YES		NULL	
q_ns1	varchar(25)	YES		NULL	
q_ns2	varchar(25)	YES		NULL	
q_ns3	varchar(25)	YES		NULL	
q_nsip1	varchar(15)	YES		NULL	
q_nsip2	varchar(15)	YES		NULL	
q_nsip3	varchar(15)	YES		NULL	
q_mx1	varchar(25)	YES		NULL	
q_mx2	varchar(25)	YES		NULL	
q_mx3	varchar(25)	YES		NULL	
q_mxip1	varchar(15)	YES		NULL	
q_mxip2	varchar(15)	YES		NULL	
q_mxip3	varchar(15)	YES		NULL	
q_mxpr1	int(11)	YES		NULL	
q_mxpr2	int(11)	YES		NULL	
q_mxpr3	int(11)	YES		NULL	
q_isp	varchar(10)	YES		NULL	
q_comments	text	YES		NULL	
q_emailto	varchar(50)	YES		NULL	
q_nons	char(1)	YES		NULL	
q_letter	char(1)	YES		NULL	
q_payment	char(1)	YES		NULL	
q_template	char(1)	YES		NULL	
q_result	char(1)	YES		NULL	
q_orig_date	date	YES		NULL	
q_mod_date	date	YES		NULL	
q_last_rev	int(11)	YES		NULL	
q_orig_by	varchar(30)	YES		NULL	
q_last_by	varchar(30)	YES		NULL	
q_reminded	char(1)	YES		NULL	
q_remindon	date	YES		NULL	
q_emailed	char(1)	YES		NULL	



University of Moratuwa, Sri Lanka.
Electronic Theses & Dissertations
www.lib.mrt.ac.lk



Onlreq Table

Field	Type	Null	Key	Default	Extra
q_domain	varchar(50)				
q_name	varchar(100)				
q_org_desc	varchar(100)	YES		NULL	
q_reason_for_selecting	varchar(100)	YES		NULL	
q_admincont	varchar(100)	YES		NULL	
q_aaddr	varchar(200)	YES		NULL	
q_atel	varchar(50)	YES		NULL	
q_afax	varchar(25)	YES		NULL	
q_ameail	varchar(50)	YES		NULL	
q_techcont	varchar(100)	YES		NULL	
q_taddr	varchar(200)	YES		NULL	
q_ttel	varchar(50)	YES		NULL	
q_tfax	varchar(25)	YES		NULL	
q_temail	varchar(50)	YES		NULL	
q_billcont	varchar(100)	YES		NULL	
q_baddr	varchar(200)	YES		NULL	
q_btetel	varchar(50)	YES		NULL	
q_btfax	varchar(25)	YES		NULL	
q_bemail	varchar(50)	YES		NULL	
q_ns1	varchar(25)	YES		NULL	
q_ns2	varchar(25)	YES		NULL	
q_ns3	varchar(25)	YES		NULL	
q_nsip1	varchar(15)	YES		NULL	
q_nsip2	varchar(15)	YES		NULL	
q_nsip3	varchar(15)	YES		NULL	
q_rr1	varchar(40)	YES		NULL	
q_rr2	varchar(40)	YES		NULL	
q_rr3	varchar(40)	YES		NULL	
q_comments	text	YES		NULL	
q_emailto	varchar(50)	YES		NULL	
q_date	datetime	YES		NULL	
q_from	varchar(15)	YES		NULL	
q_processed	char(1)	YES		NULL	



University of Moratuwa Sri Lanka
 Electronic Theses & Dissertations
www.lib.mrt.ac.lk



Dreq_rev Table

Field	Type	Null	Key	Default	Extra
qr_domain	varchar(50)				
qr_revision	int(11)			0	
qr_name	varchar(100)				
qr_org_desc	varchar(100)	YES		NULL	
qr_reason_for_selecting	varchar(100)	YES		NULL	
qr_admincont	varchar(100)	YES		NULL	
qr_aaddr	varchar(200)	YES		NULL	
qr_atel	varchar(50)	YES		NULL	
qr_afax	varchar(25)	YES		NULL	
qr_aemail	varchar(50)	YES		NULL	
qr_techcont	varchar(100)	YES		NULL	
qr_taddr	varchar(200)	YES		NULL	
qr_ttel	varchar(50)	YES		NULL	
qr_tfax	varchar(25)	YES		NULL	
qr_temail	varchar(50)	YES		NULL	
qr_billcont	varchar(100)	YES		NULL	
qr_baddr	varchar(200)	YES		NULL	
qr_bt看el	varchar(50)	YES		NULL	
qr_bfax	varchar(25)	YES		NULL	
qr_bemail	varchar(50)	YES		NULL	
qr_ns1	varchar(25)	YES		NULL	
qr_ns2	varchar(25)	YES		NULL	
qr_ns3	varchar(25)	YES		NULL	
qr_nsip1	varchar(15)	YES		NULL	
qr_nsip2	varchar(15)	YES		NULL	
qr_nsip3	varchar(15)	YES		NULL	
qr_mx1	varchar(25)	YES		NULL	
qr_mx2	varchar(25)	YES		NULL	
qr_mx3	varchar(25)	YES		NULL	
qr_mxip1	varchar(15)	YES		NULL	
qr_mxip2	varchar(15)	YES		NULL	
qr_mxip3	varchar(15)	YES		NULL	
qr_mxpr1	int(11)	YES		NULL	
qr_mxpr2	int(11)	YES		NULL	
qr_mxpr3	int(11)	YES		NULL	
qr_isp	varchar(10)	YES		NULL	
qr_comments	text	YES		NULL	
qr_letter	char(1)	YES		NULL	
qr_payment	char(1)	YES		NULL	
qr_template	char(1)	YES		NULL	
qr_mod_date	datetime	YES		NULL	
qr_mod_by	varchar(30)	YES		NULL	



University of Moratuwa, Sri Lanka.
Electronic Theses & Dissertations
www.lib.mrt.ac.lk

Pannel Table

Field	Type	Null	Key	Default	Extra
p_domain	varchar(50)		PRI		
p_reason	varchar(50)	YES		NULL	
p_result	char(1)	YES		NULL	
p_date_of_receipt	date	YES		NULL	
p_date_of_result	date	YES		NULL	
p_comment	text	YES		NULL	

Rejects Table

Field	Type	Null	Key	Default	Extra
r_domain	varchar(50)		PRI		
r_name	varchar(100)	YES		NULL	
r_reason	text	YES		NULL	
r_date	date	YES		NULL	

Users Table

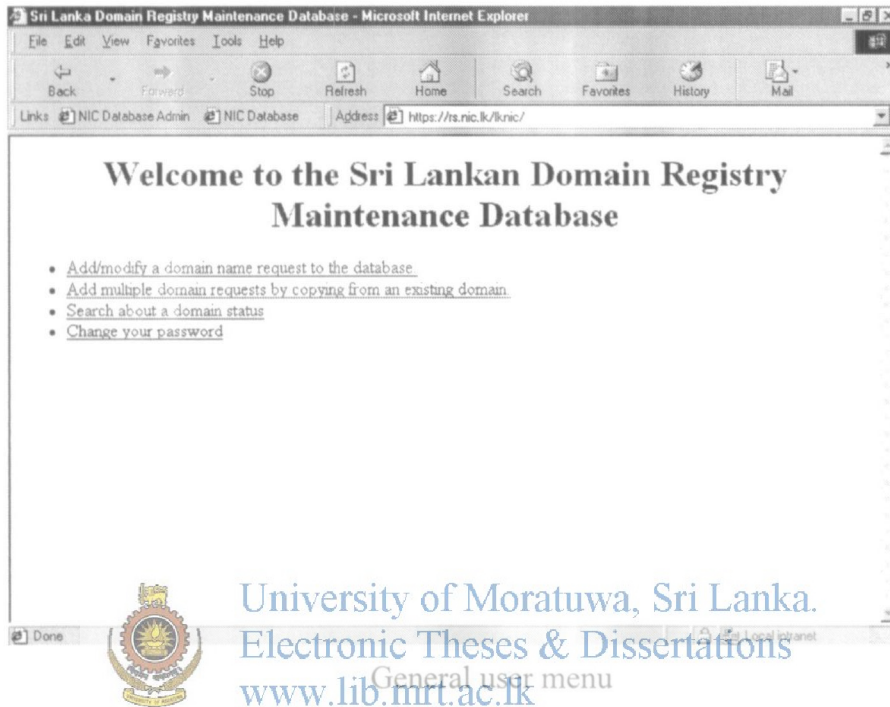
Field	Type	Null	Key	Default	Extra
userid	char(10)	YES		NULL	
abbr	char(2)	YES		NULL	
username	char(50)	YES		NULL	



University of Moratuwa, Sri Lanka.
Electronic Theses & Dissertations
www.lib.mrt.ac.lk



APPENDIX D - SCREEN SHOTS



Sri Lanka Domain Registry Maintenance Database - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites History Mail

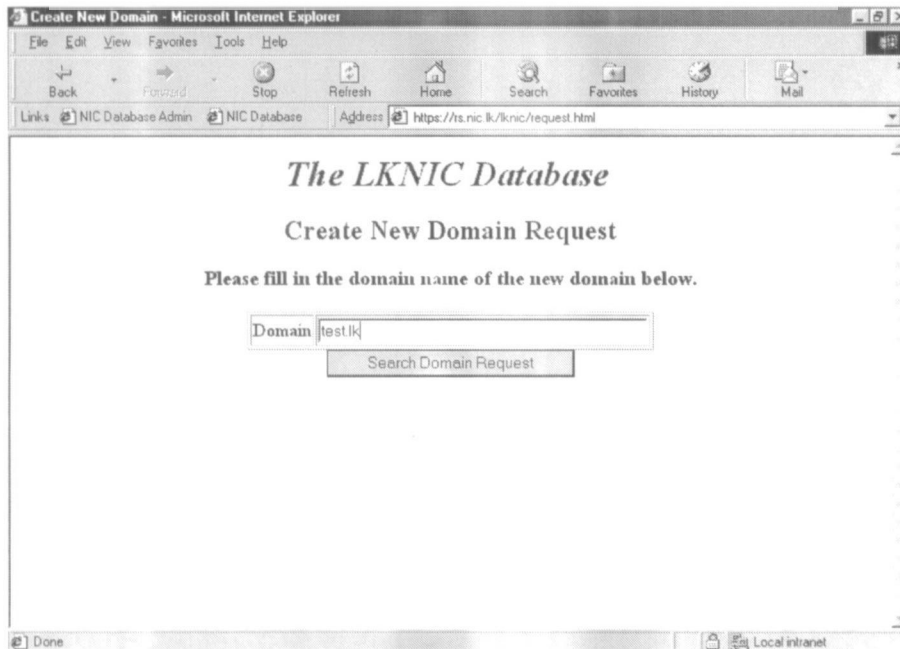
Links NIC Database Admin NIC Database Address: https://rs.nic.lk/krnic/

Welcome to the Sri Lankan Domain Registry Maintenance Database

- [Add/modify a domain name request to the database.](#)
- [Add multiple domain requests by copying from an existing domain.](#)
- [Search about a domain status](#)
- [Change your password](#)

Done

University of Moratuwa, Sri Lanka.
Electronic Theses & Dissertations
www.lib.mrt.ac.lk
General user menu



Create New Domain - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites History Mail

Links NIC Database Admin NIC Database Address: https://rs.nic.lk/krnic/request.html

The LKNIC Database

Create New Domain Request

Please fill in the domain name of the new domain below.

Domain

Done Local intranet

Domain request creation - initial

Domain Request Creation - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites History Mail

Links NIC Database Admin NIC Database Address https://rs.nic.lk/cgi-bin/parsereq.cgi

The LKNIC Database

Domain Request search Result

Please fill in the details of the new domain below.

Domain	test.lk
Name	test domain
Description	hskdjf
Reason for Selecting	ksdjf
If informed by email, email address	rasikaa@cse.mrt.ac.lk
Administrative Contact	test admin
Address	jhbgb jdkjgghd
Telephone	

Done Local intranet


Domain request creation - detail

Multiple Domain Request Creation - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites History Mail

Links NIC Database Admin NIC Database Address https://rs.nic.lk/cgi-bin/parsereqmult.cgi



University of Moratuwa, Sri Lanka.
Electronic Theses & Dissertations
www.lib.mrt.ac.lk

The LKNIC Database

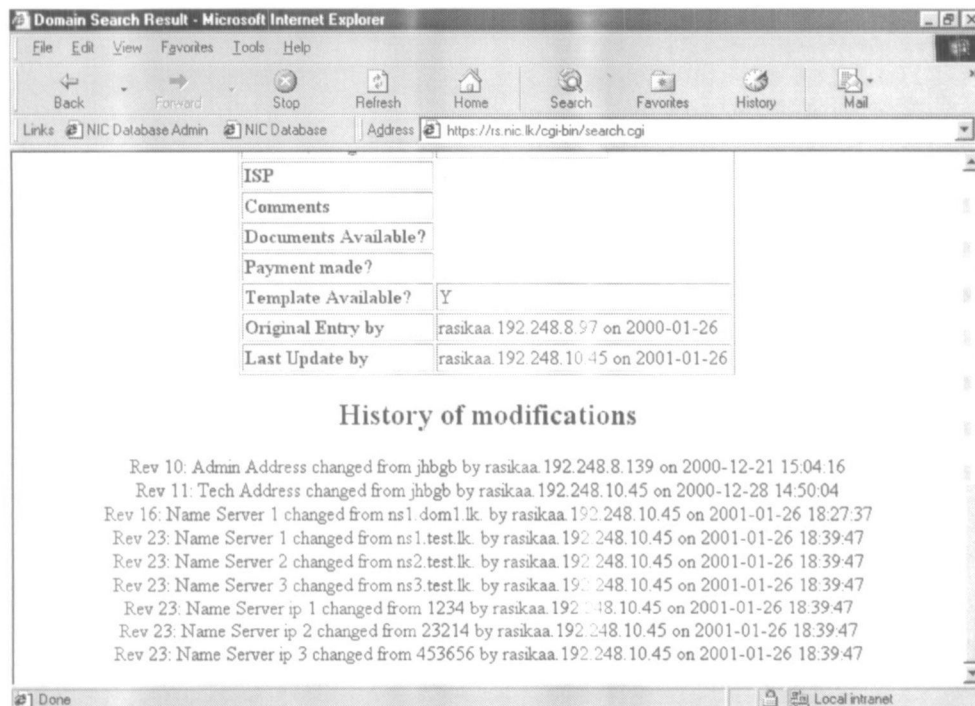
Please fill in the names of the new domains below. Start from the first and don't leave any blank domains in the middle.

Domain 1	test2.lk
Domain 2	
Domain 3	
Domain 4	
Domain 5	
Domain 6	
Domain 7	
Domain 8	
Domain 9	
Domain 10	

Done Local intranet

Multiple domain registration





Change history in a domain request



Admin user menu

Domain Request Processing - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites History Mail

Links NIC Database Admin NIC Database Address https://rs.nic.lk/cgi-bin/admin/verify_req.cgi

The LKNIC Database

List of Domains Waiting for Registration

Domain Name	Organization Name	Reason for Selecting	Letter	Payment	Template	Action to take
appstatassn.lk	Applied Statistics Association of Sri Lanka	Applied Statistics Association is a professional body. It is planning to use this website to promote	Y		Y	<input type="button" value="Process"/>
aiwa.lk	Aiwa Singapore Ltd	For our subsidiary in Sri Lanka	Y		Y	<input type="button" value="Process"/>
wizard.lk	Wizard Software				Y	<input type="button" value="Process"/>
switcher.lk	Tabell SA	switcher is the Trademark for the			Y	<input type="button" value="Process"/>

Done Local intranet

Domain processing

Processing Validated Domains - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites History Mail

Links NIC Database Admin NIC Database Address https://rs.nic.lk/cgi-bin/admin/process.cgi

The LKNIC Database

List of Domains Being Processed

Domain Name	Organization Name	Reason for Selecting
tqb.lk	Ministry of Industrial Development	
newconnection.lk	ETransMec pte. Ltd	

Entries for the domains

```

tqb          TXT      "Ministry of Industrial Development"      ; 01/02/05
            NS       parakum.evisl.net.
            NS       gajaba.evisl.net.

; newconnection - ETransMec pte. Ltd          01/02/01
; Roshan Sooriyabandara

```

Done Local intranet

Domain resource records created



REFERENCES

1. The OpenCA Project <http://www.openca.org>.
2. Thawte Certification Authority <http://www.thawte.com>.
3. Verisign Certification Authority <http://www.verisign.com>.
4. RFC 882 - *Domain Names: Concepts and Facilities*.
5. RFC 883 - *Domain names: Implementation Specification*.
6. RFC 1034 - *Domain Names: Concepts and Facilities*.
7. RFC 1035 - *Domain names: Implementation Specification*.
8. RFC 1591 - *Domain Name System: Structure and Delegation*.
9. Albitz, P. and Liu, C., DNS and BIND. *O'Rielly & Associates*, 1998.
10. Mirando, B.A, Critical Analysis of the Provisions Governing Trademarks Under the Code of Intellectual Property Act No. 52 of 1979, *Witha Yapa*, 1999.
11. Lite & w3-mSQL <http://www.hughes.com.au/library/lite/>.
12. The MySQL Project <http://www.mysql.com>.
13. The Comprehensive Perl Archive Network <http://www.cpan.org>.
14. Hell's Kitchen Systems <http://www.fks.net>.
15. Planet Payment <http://www.planetpayment.com>.
16. AuthorizeNet <http://www.authorizenet.com>.
17. CS4601 - Computer Security. A course by the US Navy on computer security issues. <http://www.cs.nps.navy.mil/curricula/tracks/security/notes/cs4601.notes.contents.html>.
18. Amarasiri, R., and Dias, G.: Techniques for Secure Electronic Transactions, In *Proceedings of the ERU Symposium, University of Moratuwa*, pp272-284, 1999.
19. Feghhi, J., Feghhi, J. and Williams, P. Digital Certificates – Applied Internet Security, *Addison Wesley*, 1998.
20. Ghosh, A.K, E-Commerce Security: weak links, best defenses, *Wiley Computer Publishing*, 1998.
21. First Virtual <http://www.fv.com>.



22. CyberCash <http://www.cybercash.com>.
23. Drew, Grady N., Using SET for secure electronic commerce, *Prentice Hall*, 1999.
24. MasterCard International - What is SET?
<http://www.mastercard.com/shoponline/set/set.html>.
25. The MilliCent™ microcommerce Network <http://www.millicent.com>.
26. eCash Solutions <http://www.digicash.com>.
27. CyberCash <http://www.cybercash.com>.
28. Mondex International <http://www.mondex.com>.
29. Introduction to SSL. <http://developer.netscape.com/docs/manuals/security/ssl/>.
30. The SSL Protocol Specification <http://www.netscape.com/eng/ssl3/>.



University of Moratuwa, Sri Lanka.
Electronic Theses & Dissertations
www.lib.mrt.ac.lk

