PKI Based Infrastructure for Secure Web Services

A project work undergone in partial fulfillment of Masters Program in IT specializing in Network Technology at Symbiosis Center for IT.

Project Guide:
Prof. Anjali Gajendragadkar

Submitted by:

D.R.Esesve (IT032022)
Varun Chaudary (IT032073)
Shalini Gupta (IT023060)
Gaurav Benjamin (IT023010)

Symbiosis Center for Information Technology
Rajiv Gandhi Infotech Park, Pune
www.scit.edu

ACKNOWLEDGEMENTS

We express our heartfelt gratitude to our project guide Prof. Anjali Gajendradakar, who has helped us in completing this project very well. She has provided the insight of all the aspects of the project. Her assistance is invaluable.

We also would like to thank our Network Administrator, Lab Faulty and other staff who have helped us all through our project.

We would like to thank our director for providing immense resources like the library and laboratory which helped us experiment every possible aspect of the implementation.

We are also thankful to our senior Miss. Rupali Anand who has helped us acquiring knowledge about some of the issues of the PKI. Her support was really commendable

Contents

ABSTRACT

1. Abstract

Electronic data communication is omnipresent in this e-world. Both parties involved need to trust one another, authenticated and transactions should be secure. The better solution for such transaction is Public Key Infrastructure. This was found out by Mr. Diffie and Mr. HellMan in 1976. In 1978 in the paper "*A Method for Obtaining Digital Signatures and Public Key Cryptosystems*" Rivest, Shamir, and Adleman proposed a particular implementation of the Diffie-HellMan concept.

This project is the implementation of the same model for secure e-commerce applications. A Certificate authority (CA) is created which helps in secure communication and proper authentication. The CA provides both the server and the client certificates with which one can authenticate the other. Also the pros and cons of the project findings have been listed and studied upon.

2. INTRODUCTION

2. Introduction

Billions of dollars are spent on computer security. The people who break cryptographic systems don't follow rules; they cheat. They can attack a system using techniques the designers never thought of. Art thieves have burgled homes by cutting through the walls with a chain saw. Home security systems, no matter how expensive and sophisticated, won't stand a chance against this attack. Computer thieves come through the walls too. They steal technical data, bribe insiders, modify software, and collude. The odds favor the attacker: defenders have to protect against every possible vulnerability, but an attacker only has to find one security flaw to compromise the whole system.

Present-day computer security is a house of cards; it may stand for now, but it can't last. No one can guarantee 100% security. But we can work toward 100% risk acceptance. Fraud exists in current commerce systems: cash can be counterfeited, checks altered, credit card numbers stolen. Yet these systems are still successful because the benefits and conveniences outweigh the losses. Privacy systems -- wall safes, door locks, curtains -- are not perfect, but they're often good enough. A good cryptographic system strikes a balance between what is possible and what is acceptable.

With businesses spreading all over the globe, the transactions are now done on the internet. Thus authentication of users and integrity of data has become highly crucial.

2.1 Issues of security in e-Commerce

In every transaction, both the individuals should be confident of the other person, who is transacting. In conventional cryptography, there used to be one secret key with which two individuals used to validate one another.

This cannot be a possibility when the boundaries of the businesses are global. The number of users transacting with an entity or organization is huge. Thus maintaining private keys with every user cannot be done. Also key management would be a tough issue.

Cryptography has provided us with digital signatures that resemble in functionality the hand–written signatures and digital certificates that relate to an ID card or some other official document. However, in order to use these technologies, we need to make the necessary provisions so that their usage is equally transparent and secure. The Public Key Infrastructures along with the Privileged Management Infrastructure are candidates to aid this transparency and security of applications of the Internet.

2.2 The Risks and Challenges of E-Commerce Trust

To succeed in the fiercely competitive e-commerce marketplace, businesses must become fully aware of Internet security threats, take advantage of the technology that overcomes them, and win customers' trust. By becoming aware of the risks of Internet-based transactions, businesses can acquire technology solutions that overcome those risks. The risks can be spoofing, unauthorized disclosure, unauthorized action, eavesdropping, and data alteration.

The above risks can be because of the following:

1. Bugs or misconfiguration problems in the Web server. This allows unauthorized remote users to:
   - Steal confidential documents not intended for their eyes.
   - Execute commands on the server host machine, allowing them to modify the system.
   - Gain information about the Web server's host machine that will allow them to break into the system.
   - Launch denial-of-service attacks, rendering the machine temporarily unusable.
2. Browser-side risks, including:
   - Active content that crashes the browser, damages the user's system, breaches the user's privacy, or merely creates an annoyance.
   - The misuse of personal information knowingly or unknowingly provided by the end user.
3. Interception of network data sent from browser to server or vice versa via network eavesdropping. Eavesdroppers can operate from any point on the pathway between browser and server including:
   - The network on the browser’s side of the connection.
   - The network on the server’s side of the connection (including intranets).
   - The end-user’s Internet service provider (ISP).

- The server's ISP.
- Either ISP's regional access provider.

The solution for tackling the problems mentioned above includes two essential components:

1. Digital certificates for Web servers, to provide authentication, privacy and data integrity through encryption.
2. A secure online payment management system, to allow e-commerce Web sites to securely and automatically accept, process, and manage payments online

Together, these technologies form the essential trust infrastructure for any business that wants to take full advantage of the Internet

Public-key cryptography provides three capabilities that are especially valuable to businesses. First, it provides privacy for data. Second, it allows robust identification, or *authentication*, of users and machines. Finally, it provides non-repudiation—the ability to prove that someone took a particular action.

3. PKI Solution for secure E-Commerce

3. PKI – Solution for secure e-Commerce

Public Key Infrastructure is a technology introduced by Diffie and Hellman in 1976. PKI is the acronym for Public Key Infrastructure. The technology is called Public Key because unlike earlier forms of cryptography it works with a pair of keys. One of the two keys may be used to encrypt information which can only be decrypted with the other key. One key is made public and the other is kept secret. The secret key is usually called the private key. Since anyone may obtain the public key, users may initiate secure communications without having to previously share a secret through some other medium with their correspondent. The Infrastructure is the underlying systems needed to issue keys and certificates and to publish the public information.

PKI is a security architecture that has been introduced to provide an increased level of confidence for exchanging information over an increasingly insecure Internet. PKI facilities can, however, be used just as easily for information exchanged over private networks, including corporate internal networks.

PKI can also be used to deliver cryptographic keys between users (including devices such as servers) securely, and to facilitate other cryptographically delivered security services. Technically, PKI refers to the technology, infrastructure, and practices that support the implementation and operation of a certificate-based public key cryptographic system. Thus, Public-key cryptography is crucial for e-commerce, internet, intranet and other applications that require *distributed security* — security in which the participants are not part of the same network and have no common security credentials.

In a context of globalization, computerized exchanges are becoming more and more necessary, even essential, for successful relationship in B2B, C2A or B2A. The confidentiality of these exchanges is based on a good encoding of the data, and in particular on infrastructures such as public keys (**PKI**).

PKI is a security architecture that has been introduced to provide an increased level of confidence for exchanging information over an increasingly insecure Internet. A PKI is the set of operating system and application services that make it easy and convenient to use public-key cryptography. Public-key cryptography uses a pair of mathematically related cryptographic keys.

If one key is used to encrypt information, then only the related key can decrypt that information. If you know one of the keys, you cannot easily calculate what the other one is.

There are two fundamental operations associated with public key cryptography: encryption and signing. The goal of encryption is to obscure data in such a way that it can only be read by the intended party. Digital IDs address this problem, providing an electronic means of verifying someone's identity. Used in conjunction with encryption, Digital IDs provide a more complete security solution, assuring the identity of all parties involved in a transaction. A PKI gives the ability to manage keys, Publish keys, Use keys. Once these capabilities exist, application developers can use them to build more secure applications. However, those applications depend on having a secure, easy-to-use, flexible way to manage, publish, and use public keys—that's where the PKI comes in.

An enterprise PKI uses digital certificates to protect information assets via the following mechanisms:

- Authentication
- Encryption
- Digital signing
- Access control
- Non-repudiation

3.1 Public Key Certificates

A public key needs to be associated with the name of its owner. This is done using a public key certificate, which is a data structure containing the owner's name, their public key and e-mail address, validity dates for the certificate, the location of revocation information, the location of the issuer's policies and possibly other information such as their affiliation with the certificate issuer (often an employer or institution). The certificate data structure is signed with the private key of the issuer so that a recipient can verify the identity of the signer and prove that data in the certificate has not been altered. Public Key Certificates are then published, often in an LDAP directory, so that users of the PKI can locate the certificate for an individual with whom they wish to communicate securely.

4. Implementation of PKI

4. Implementation of PKI

Public Key Infrastructure, implementation was carried out as the project.

4.1 Scope

The criteria of the project are as follows.

- ✓ Installing and configuring a Certificate authority server
- ✓ Installing and configuring a Web server
- ✓ Issuing Certificates to the web server
- ✓ Issuing Certificates to clients
- ✓ Authenticating both Servers and clients
- ✓ Ensuring that communication is secure
- ✓ Testing all these modules

The project implements the well known PKI infrastructure. There would not be a tier of implementation of CA.

4.2 Literature Survey

An enormous amount of literature survey and study of the same has been conducted before the start of the project. The major resources were the Internet and the library of SCIT. Some of them have been listed and their findings are listed below.

I. Ten Risks of PKI – Bruce Schneier & Carl Ellision

II. Federal Information Processing Standards Publication – FIPS
    a. FIPS Pub – 112 on Password Usage
    b. FIPS Pub – 31 on Automatic Data Processing, Physical security and risk management
    c. FIPS Pub – 186-2 on Digital Signature Standards
    d. FIPS Pub – 196 on Entity Authentication using Public Key Cryptography
    e. FIPS Pub – 140-1 on Security requirements for Cryptographic Models
    f. FIPS Pub – 102 on Guidelines for Computer Security Certification and accreditation

III. NIST special Publication 800-25 for Use of Public Key Technology for Digital Signatures and authentication

Some of these documents said that Digital Signatures, Certificates are the way these days Businesses are done. However, there were enough critiques who had the opinion that “its not e-commerce that is living on PKI, moreover its PKI which entirely depends on e-commerce”. The literature survey helped the project, work in a direction, where we could understand the broad spectrum of PKI, pros and cons.

4.3 Requirements

The following technologies and products were required and thus used in the implementation of Public Key Infrastructure.

i. A server OS was required which could provide us a CA server and web server was required. Thus Microsoft Windows 2000 Server Used.
ii. A client OS was required to be used as a client. Thus Microsoft Window 2000 Professional was used.
iii. Licensed copies of both these Operating Systems have been provided by the college.
iv. Ethereal, a packet filter over the network was used. This is a freeware available on the net.

4.4 Installation and Configuration of Certificate Authority Server

Microsoft Windows 2000 Advanced server comes with the required Certificate Authority Module. After the installation of the OS, it has to be installed separately.

4.4.1 Configuration of the Microsoft Windows 2000 PKI

The PKI is contained in the program package of the Windows 2000 Advanced server. The PKI was used in an environment without Active Directory. If one were to use this PKI with Active Directory, only the display of the certificates changes. In an Active Directory environment the certificate would be issued automatically by the request for the certificate.

Logging in automatically authenticates the user into the domain. If one would like to use the PKI outside an Active Directory environment, the administrator can decide to issue the certificate manually or automatically.

4.4.2 Installing PKI

For the CA server to issue a certificate meeting the minimum key length requirement of the Challenge (1024 bits), the CA server certificate must have that or longer key length.
After installing and configuring the Windows 2000 Advanced server, an administrator can add a CA:

Step 1 Select System control -> Software -> Add/ Remove Windows components

The administrator selects the certificate services and gets the following message:
"After installing the certificate services the computer cannot be renamed nor can a domain be joined or removed. Would like you to continue the occurrence?"

This message is confirmed with yes and the administrator sees a checkmark in the Certificate Authority box.

To install the certificate services, the administrator clicks on Next
On the next screen, the administrator can select the features of a CA to install:

- ✓ Root Certificate Authority
- ✓ Subordinated Certificate Authority

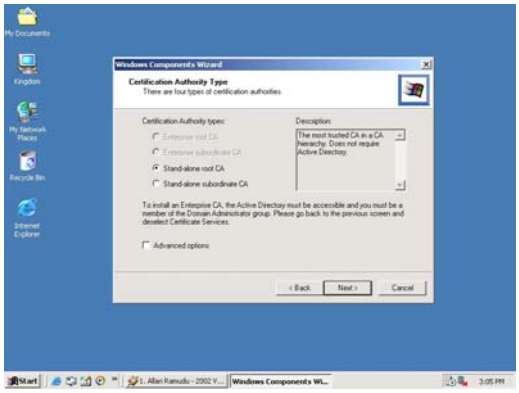


Figure 1

At this screen, one can also select to operate the CA within an organization, under use of Active Directory, or as an independent CA.

Before proceeding further, one should click on the expanded option button. There one can select the Cryptographic module, the Hash algorithms for the certificate of the CA and most important the key length. Also one has the possibility to bind to an already available certificate (of a trusted organization).

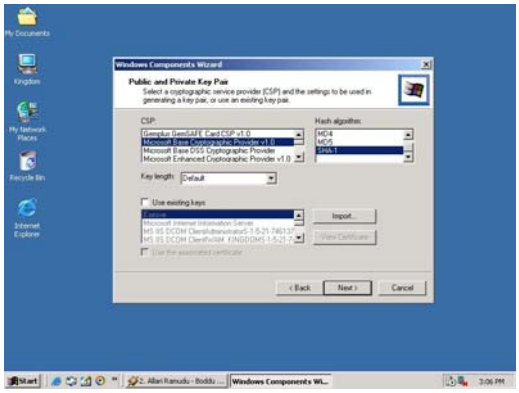


Figure 2

After choosing the key length and the algorithm, a page comes up on which one can specify CA more closely.

On that page one enters the following information:

- CA name
- Name of the organization responsible for the CA
- City, state and the country of the organization
- email address of the CA

In addition, one can indicate a short description of the Certificate Authority. If constructing a root CA, one must indicate expiration or the validity duration of the CA certificates. In constructing a subordinated CA, the root CA determines the validity of the subordinate CA certificates.

Step 1 Confirm requests by expanding the window

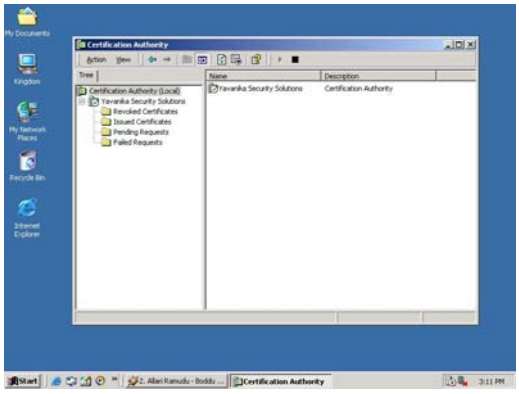
Step 2 Determine the storage location of the certificates in the next window

One can use the default certificate storage Microsoft provides or specify a certificate database at another storage location.

With the final click on Next, one configures the Certificate Authority, generates the accompanying certificate, and stores it in the certificate storage indicated previously.

4.4.3 Configuration of the Certificate Authority

Once after the installation of the Certificate Authority, it could be started it under
Start -> Programs -> Administration -> Certificate Authority.



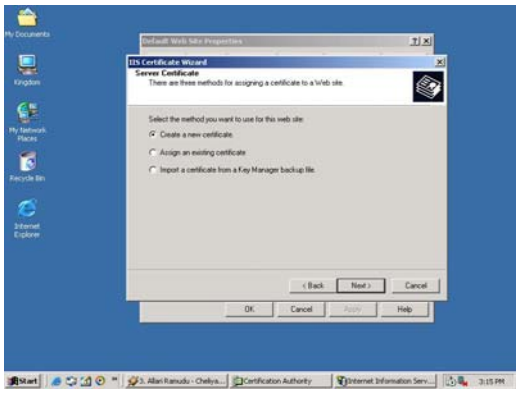
At this screen, one has different selection possibilities:

1. "Blocked Certificates" folder—Blocked Certificates with the reason for the block (if a reason is indicated)
2. "Issued Certificates" folder—Certificates the CA issues
3. "Certificate Requests" folder—If a CA is configured without Active Directory, the CA administrator must issue the certificates
4. "Failed Requests" folder—Requests that were rejected for any reason
5. "Adjustments" folder—Guidelines for adjusting the CA

Mark the adjustments on the Certificate Authority folder and then right click.
A new window will open where you can choose the desired adjustments of the PKI.

4.4.4 Certificate Request

The request of a certificate takes place via Web browser by opening the URL http://server/certsrv.
When the window is open, select request a new certificate.



On the next page, select expanded requests.

After that click "Send a Certificate Request" to this Certificate Authority

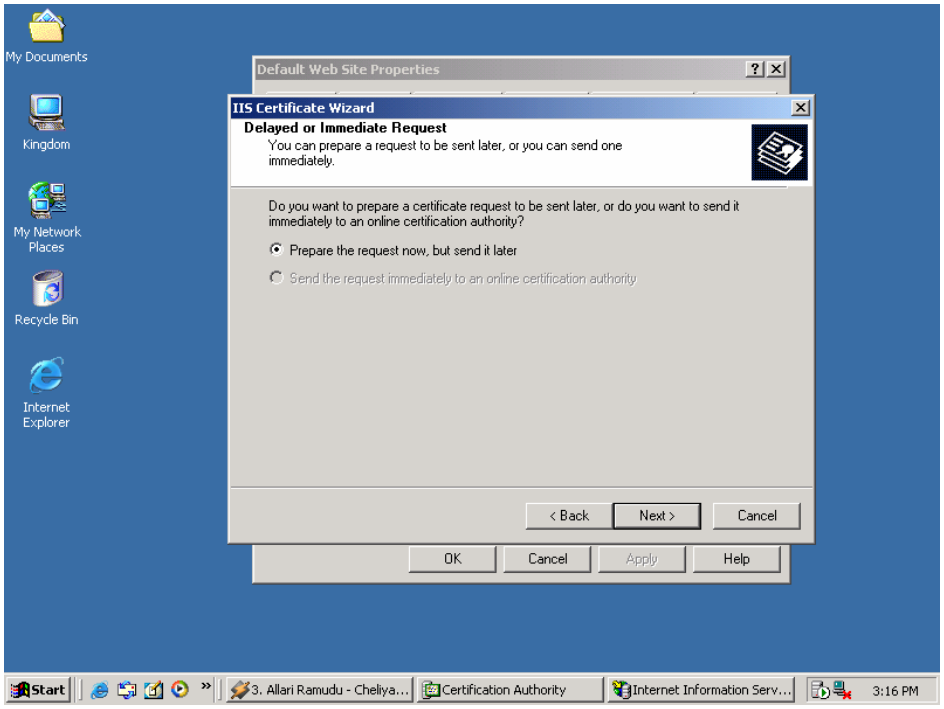
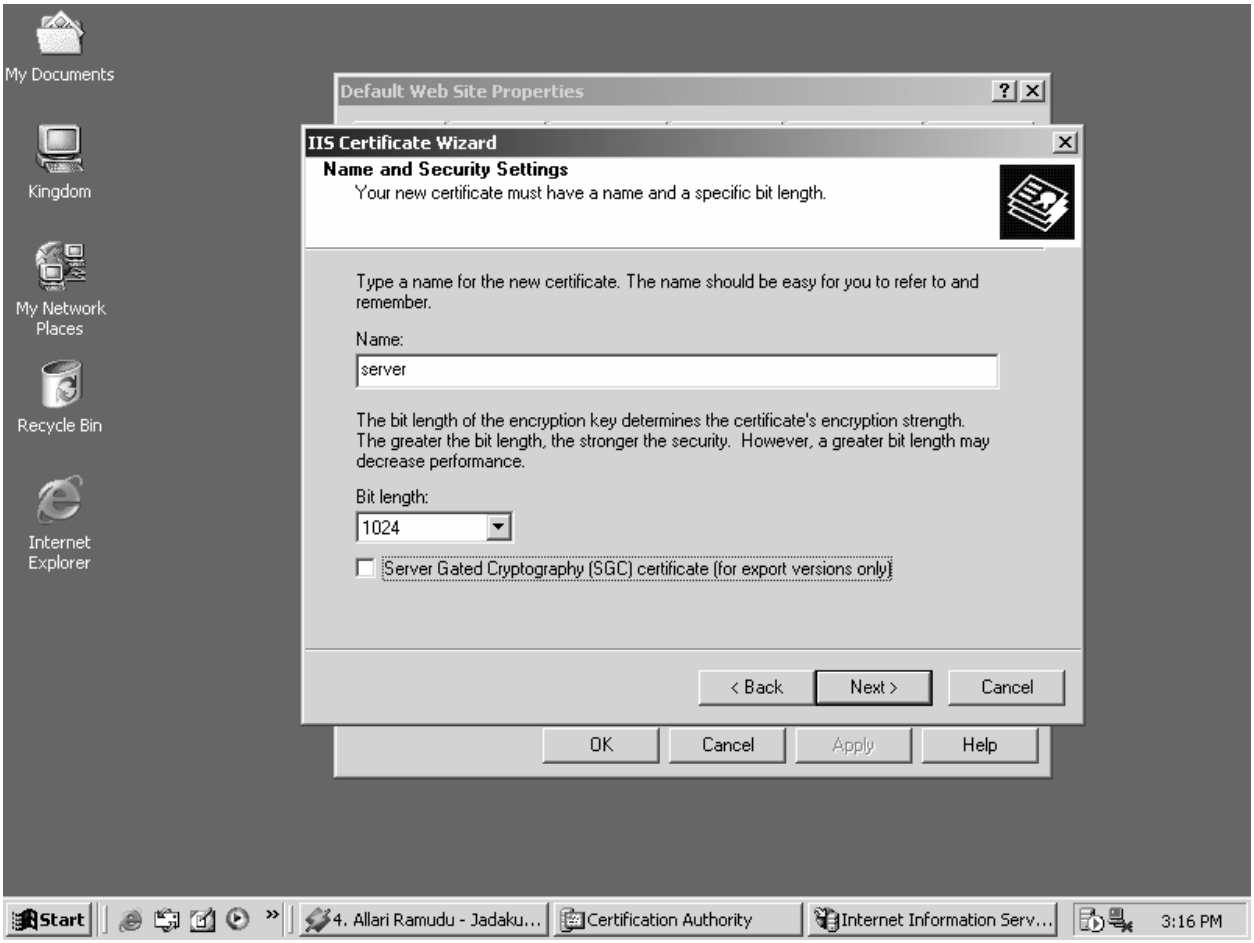


Figure 3

On the next page:

Step 1 Input the user's data—Purpose for the certificates is an email protection certificate

Step 2 Select the key options—OK to select the default key provider



Step 3 Set the key length on 1024-bit to enable the tightest security

Step 4 Generate a new key pair that activates the enhanced security and is marked "for export"

Note: The key is not exported into a file, but rather stored in the certificate. Lotus Notes can bind to this. In the additional options, SHA-1 must be adjusted as a Hash algorithm before submitting the request.

After pushing the Send Button, a message appears that the middle security step was selected.

Set the security step on high. After sending the request to the server, the extensive security examinations (see also CP and CPS) are fulfilled and the certificate is issued to the certificate requester.

To pick up the issued certificate, go to http://server/certsrv, where the outstanding certificate is marked.

Step 1 Select Next—User sees all the requested certificates that have been issued
Step 2 Select the appropriate certificate
Step 3 Go to "install this certificate"—Installs automatically in the certificate storage of Microsoft Windows 2000

4.5 Installation and Configuration of Web Server

Microsoft Windows 2000 Server comes with a web server, Internet Information Services 5.0. Upon installation of the Operating System the web server gets installed. The utility comes with a default website, a default ftp site and a default SMTP service.

4.5.1 Installing IIS

Internet Information Services is installed on Windows 2000 Server by default. You can remove IIS or select additional components by using the Add/Remove Programs application in Control Panel.

To install IIS, add components, or remove components

Click Start, point to Settings, click Control Panel and start the Add/Remove Programs application.

Select Configure Windows, click the Components button, and then follow the on-screen instructions to install, remove, or add components to IIS.
Note If upgraded to Windows 2000, IIS 5.0 will be installed by default only if IIS was installed on your previous version of Windows.

4.5.2 Quick Site Setup with IIS

IIS creates a default Web site and FTP site when you install Windows 2000 Server. This topic describes how to publish information on those default sites.

4.5.2.1 To publish content on your Web site

Create a home page for your Web site. See Choosing an Authoring Tool for more information on available tools used in Web site creation.
Name your home page file Default.htm or.

Copy your home page into the default Web publishing directory for IIS. The default Web publishing directory is also called the home directory, and the location provided by Setup is \Inetpub\Wwwroot.

If your network has a name resolution system (typically DNS), then visitors can simply type your computer name in the address bar of their browsers to reach your site. If your network does not have a name resolution system, then visitors must type the numerical IP address of your computer. For more information, see About Name Resolution.

4.5.2.2 To publish content on your FTP site

Copy or move your files into the default FTP publishing directory. The default directory provided by Setup is \Inetpub\Ftproot.

If your network has a name resolution system (typically DNS), then visitors can type ftp:// followed by your computer name in the address bar of their browsers to reach your site. If not, then visitors must type ftp:// and the numerical IP address of your computer. To customize the appearance of your FTP site, see Setting FTP Messages and Directory Output Style.
To add additional Web or FTP sites to your computer

Review the conceptual information that describes hosting multiple sites on one computer in the section hosting Multiple Sites by Assigning Ports, Addresses, and Host Header Names in the About Name Resolution topic.

4.5.3 Features of IIS

Internet Information Services 5.0 has many new features to help Web administrators to create scalable, flexible Web applications.

- ✓ Security
- ✓ Administration
- ✓ Programmability
- ✓ Internet Standards

4.5.3.1 Security

- Digest Authentication: Digest authentication allows secure and robust authentication of users across proxy servers and firewalls. In addition, Anonymous, HTTP Basic, and integrated Windows authentication (formerly known as Windows NT Challenge/Response authentication and NTLM authentication) are still available.
- Secure Communications: Secure Sockets Layer (SSL) 3.0 and Transport Layer Security (TLS) provide a secure way to exchange information between clients and servers. In addition, SSL 3.0 and TLS provide a way for the server to verify who the client is before the user logs on to the server. In IIS 5.0, client certificates are exposed to both ISAPI and Active Server Pages, so that programmers can track users through their sites. Also, IIS 5.0 can map the client certificate to a Windows user account, so that administrators can control access to system resources based on the client certificate.
- Server-Gated Cryptography: Server-Gated Cryptography (SGC) is an extension of SSL that allows financial institutions with export versions of IIS to use strong 128-bit encryption. Although SGC capabilities are built into IIS 5.0, a special SGC certificate is required to use SGC.
- Security Wizards: Security wizards simplify server administration tasks.
- The Web Server Certificate Wizard simplifies certificate administration tasks, such as creating certificate requests and managing the certificate life cycle.
- The Permissions Wizard makes it easy to configure Web site access by assigning access policies to virtual directories and files. The Permissions Wizard can also update NTFS file permissions to reflect these Web access policies.
- The CTL wizard helps you configure your certificate trust lists (CTLs). A CTL is a list of trusted certification authorities (CAs) for a particular directory. CTLs are especially useful for Internet service providers (ISPs) who have several Web sites on their server and who need to have a different list of approved certification authorities for each site.

- IP and Internet Domain Restrictions: You can grant or deny Web access to individual computers, groups of computers, or entire domains.
- Kerberos v5 Authentication Protocol Compliance: IIS is fully integrated with the Kerberos v5 authentication protocol implemented in Microsoft® Windows® 2000, allowing you to pass authentication credentials among connected computers running Windows.
- Certificate Storage: IIS certificate storage is now integrated with the Windows CryptoAPI storage. The Windows Certificate Manager provides a single point of entry that allows you to store, back up, and configure server certificates.
- Fortezza: The U.S. government security standard, commonly called Fortezza, is supported in IIS 5.0. This standard satisfies the Defense Message System security architecture with a cryptographic mechanism that provides message confidentiality, integrity, authentication, and access control to messages, components, and systems. These features can be implemented both with server and browser software and with PCMCIA card hardware.

4.5.3.2 Administration

- Restarting IIS: Now you can restart your Internet services without having to reboot your computer.
- Backing Up and Restoring IIS: You can back up and save your metabase settings to make it easy to return to a safe, known state.
- Process Accounting: Provides information about how individual Web sites use CPU resources on the server. This information is useful in determining which sites are using disproportionally high CPU resources or which might have malfunctioning scripts or CGI processes.
- Process Throttling: You can limit the percentage of time the CPU spends processing out-of-process ASP, ISAPI, and CGI applications for individual Web sites. In addition, misbehaving processes can be stopped and restarted.
- Improved Custom Error Messages: Now administrators can send informative messages to clients when HTTP errors occur on their Web sites. Also includes detailed ASP error processing capabilities through the use of the 500-100.asp custom error message. You can use the custom errors that IIS 5.0 provides, or create your own.

- Configuration Options: You can set permissions for Read, Write, Execute, Script, and FrontPage Web operations at the site, directory, or file level.
- Remote Administration: IIS 5.0 has Web-based administration tools that allow remote management of your server from almost any browser on any platform. With IIS 5.0, you can set up administration accounts called Operators with limited administration privileges on Web sites, to help distribute administrative tasks.
- Terminal Services: Terminal Services is a feature of Windows 2000 that allows you to run 32-bit Windows applications on terminals and terminal emulators running on personal computers and other computer desktops. Terminal Services allows virtually any desktop to run applications on the server. This enables you to remotely administer Windows 2000 services such as IIS as if you were at the server console, including administration from older legacy PCs, or even non-PC devices such as UNIX workstations with compatible client software. (Non-Windows-based client devices require third-party add-on software.)
- Centralized Administration: Administration tools for IIS use the Microsoft® Management Console (MMC). MMC hosts the programs, called snap-ins, that administrators use to manage their servers. You can use IIS snap-in from a computer running Windows 2000 Professional to administer a computer on your intranet running Internet Information Services on Windows 2000 Server.

4.5.3.3 Programmability

- Active Server Pages: You can create dynamic content by using server-side scripting and components to create browser-independent dynamic content. Active Server Pages (ASP) provides an easy-to-use alternative to CGI and ISAPI by allowing content developers to embed any scripting language or server component into their HTML pages. ASP provides access to all of the HTTP request and response streams, as well as standards-based database connectivity and the ability to customize content for different browsers.
- New ASP Features: Active Server Pages has some new and improved features for enhancing performance and streamlining your server–side scripts.
- Application Protection: IIS 5.0 offers greater protection and increased reliability for your Web applications. By default, IIS will run all of your applications in a common or pooled

process that is separate from core IIS processes. In addition, you can still isolate mission-critical applications that should be run outside of both core IIS and pooled processes.

- ADSI 2.0: In IIS 5.0, administrators and application developers will have the ability to add custom objects, properties, and methods to the existing ADSI provider, giving administrators even more flexibility in configuring their sites.

4.5.3.4 Internet Standards

- Standards Based: Microsoft Internet Information Services 5.0 complies with the HTTP 1.1 standard, including features such as PUT and DELETE, the ability to customize HTTP error messages, and support for custom HTTP headers.
- Multiple Sites, One IP Address: With support for host headers, you can host multiple Web sites on a single computer running Microsoft Windows 2000 Server with only one IP address. This is useful for Internet service providers and corporate intranets hosting multiple sites.
- Web Distributed Authoring and Versioning (WebDAV): Enables remote authors to create, move, or delete files, file properties, directories, and directory properties on your server over an HTTP connection.
- News and Mail: You can use SMTP and NNTP Services to set up intranet mail and news services that work in conjunction with IIS.
- PICS Ratings: You can apply Platform for Internet Content Selection (PICS) ratings to sites that contain content for mature audiences.
- FTP Restart: Now File Transfer Protocol file downloads can be resumed without having to download the entire file over again if an interruption occurs during data transfer.
- HTTP Compression: Provides faster transmission of pages between the Web server and compression-enabled clients. Compresses and caches static files, and performs on-demand compression of dynamically generated files.

4.6 Working of PKI Scheme

The Certificate authority server and IIS were installed as specified. Also the certificates are issued to the IIS default website as discussed in **4.4.4**. Then the secure channel of website is configured as follows.

a) Right click on the website and choose properties.
b) The *document security* tab is selected.
c) The *edit* button is selected.
d) The document access properties are changed to secure channel and the number of bits of encryption is selected.
e) The options for client certificates can be ignored, because generally client certificates are not so extensively used because of their loop holes in security.
f) From then the webpages to be accessed should be addressed with the prefix *https://*
g) Thus from now whenever any client request for the website, a secure channel is established and data flows in encrypted form.

The methodology discussed in 4.4.4 describes about Server Authentication. Similarly the CA server can be accessed and client certificates can be requested. The CA decides whether to issued or deny. Upon issue the webserver can be configured to authenticate clients with the certificates only. Unfortunately the client has to carry the certificate wherever he has to go. Also the webserver authenticates the certificate, or to be more clear, the person who has the certificate. So if the certificate is lost or stolen then again it's a threat. That is why client certificates don't hold much importance.

Thus configuration of the web server to communicate in secure mode using PKI has been configured. The aftermath of this implementation, the findings of the project are listed in the next section.

5. Key Management

5. Key Management

One of the major roles of the public key encryption has been to address the problem of key distribution. There are actually two distinct aspect to the use of public key cryptography in this regard.

1. The distribution of Public Keys.
2. The use of public key encryption to distribute secret keys.

5.1 Distribution of Keys

Several techniques have been proposed for the distribution of public keys. Virtually all these proposals can be grouped into the following general schemes.

- Public announcement
- Publicly available directory
- Public key authority
- Public key certificates

5.1.1 Public Announcement of Public Keys

On the face of it, the point of public-key encryption is that the public key is public. Thus if there is some broadly accepted public key algorithm, such as RSA any participant can send his or her public key to any other participant of broadcast the key to the community at large. Although this approach is convenient, it has a major weakness. Anyone can forge such a public announcement. That is, some user could pretend to be user A and send a public key to another participant or broadcast such a public key. Until such time as user A discovers the forgery and alerts other participants, the forger is able to read all encrypted messages intended for A and can use the forged keys for authentication.

5.1.2 Public Available Directory

A greater degree of security can be achieved by maintaining a publicly available dynamic directory of public keys. Maintenance and distribution of the public directory would have to be

the responsibility of some trusted entity or organization. Such scheme would include the following elements.

- ✓ The authority maintains a directory with an entry (name, public key) for each participant.
- ✓ Each participant registers a public key with the directory authority. Registration would have to be in person or by some from of secure authenticated communication.
- ✓ A participant may replace the existing key with a new one at any time, either because of the desire to replace a public key that has already been used for a large amount of data, or because the corresponding private key has been compromised.
- ✓ Periodically, the authority published the entire directory or updates to the directory.
- ✓ Participants could also access the directory electronically. For such purpose, secure, authenticated communication from the authority to the participant is mandatory.

Inspite of the good features discussed this methodology has some vulnerabilities. If an opponent succeeds in obtaining or computing the private key or the directory authority, the opponent could authoritatively pass out counterfeit public keys and subsequently impersonate any participant and eavesdrop on messages sent to any participant. Another way to achieve the same end is for the opponent to tamper with the records kept by the authority.

5.1.3 Public Key Authority

Stronger security for public-key distribution can be achieved by providing tighter control over the distribution of public keys from the directory. Here also it is assumed that a central authority maintains a dynamic directory of public keys of all participants. In addition, each participant reliably knows a public key for the authority with only the authority knowing the corresponding private key.

5.1.4 Public Key Certificates

The public key authority could be somewhat of a bottleneck in the system, for a user must appeal to the authority for a public key for every other user that it wishes to contact. As before, the directory of names and public keys maintained by the authority is vulnerable to tampering.

An alternative for this would be to use **certificates** that can be used by participants to exchange keys without contacting a public-key authority, in a way that is reliable as if the keys were obtained directly from the public key authority. Each certificate contains a public key and other information, is created by a certificate authority, and is given to the participant with the matching private key. A participant conveys its key information to another by transmitting its certificate. Other participants can verify that the certificate was created by the authority. The following are the requirements.

- ✓ Any participant can read a certificate to determine the name and public key of the certificate's owner.
- ✓ Any participant can verify that the certificate originated from the certificate authority and is not counterfeit.
- ✓ Only the certificate authority can create and update certificates.
- ✓ Any participant can verify the currency of the certificate.

5.2 Conclusions on Key Management

As discussed above Key management is a tough process in the whole PKI system. As referred by Bruce Schneier, "Certificate Authority is one who maintains his private keys well". Thus, the maintenance of keys and distribution of the same is the main foundation of the whole PKI system. The above suggested methods, having their own pros and cons, help the objective of Key Management.

6. CONCLUSION

6. Conclusion

The project successfully completed the configuring of a CA Server (Root CA), and its working is tested using a web server and a client machine. Both server and client certificates are requested, issued, revoked. All the security measures for secure communication have been completed.

The above procedures and implementations complete the implementation of Public Key Infrastructure successfully in on Windows 2000 Advanced Server. The same can be extended onto different operating systems. Most of the issues remain the same even on migration.

Further perspectives of this project:

The project can be extended can be used to implement security for any local LAN, i.e. for email servers, ftp servers etc.

7. BIBLIOGRAPHY

7. Bibliography

1. Network security by Kaufman
2. TCP/IP Protocol Suite – Forouzan
3. Computer Networks by Andrew S TenanBaum
4. Ten Risks of PKI – Bruce Schneier & Carl Ellision
5. Federal Information Processing Standards Publication – FIPS
    a. FIPS Pub – 112 on Password Usage
    b. FIPS Pub – 31 on Automatic Data Processing, Physical security and risk management
    c. FIPS Pub – 186-2 on Digital Signature Standards
    d. FIPS Pub – 196 on Entity Authentication using Public Key Cryptography
    e. FIPS Pub – 140-1 on Security requirements for Cryptographic Models
    f. FIPS Pub – 102 on Guidelines for Computer Security Certification and accreditation
6. NIST special Publication 800-25 for Use of Public Key Technology for Digital Signatures and authentication
7. www.pki.org
8. www.verisign.com
9. http://www.microsoft.com/technet/security
10. www.rsa.org
11. R & D Report on Secure HTTP Services using Digital Certificates (PKI) - January 30, 2004 - Submitted By: Roopali Anand (SCIT)