DIGITAL KEY FOR WEB SITE AUTHENTICATION

MOHD. AFIQ BIN HJ AHMAD

This report is submitted in partial fulfillment of the requirement for the Bachelor of Computer Science (Computer Networking)

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
KOLEJ UNIVERSITI TEKNIKAL KEBANGSAAN MALAYSIA
2006

TESIS^ APPROVAL STATUS FORM

JUDUL: DIGITAL KEY FOR WEB SITE AUTHENTICATION

SESI PENGAJIAN: 2003/2004

Saya MOHD AFIQ BIN HJ AHMAD

mengaku membenarkan tesis (PSM/Sarjana/Doktor Falsafah) ini disimpan di Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dengan syarat-syarat kegunaan seperti berikut:

1. Tesis dan projek adalah hakmilik Kolej Universiti Teknikal Kebangsaan Malaysia.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajain tinggi.
4. **Sila tandakan (/)

_____ SULIT (Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)

_____ TERHAD (Mengandungi meklumat TERHAD yang telah ditentukan oleh organisasi/badan di mama penyelidikan dijalankan)

/ TIDAK TERHAD

(TANDATANGAN PENULIS)

Alamat tetap: TBP 1924 Jln Abd.Kadir,
14000Bukit Mertajam,
Pulau Pinang

Tarikh: 22 NOV 2006

(TANDATANGAN PENYELIA)

Pn. Siti Rahayu Bt Selamat
Nama Penyelia

Tarikh: 22 NOV 2006

CATATAN: ** Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa.

^ Tesis dimaksudkan sebagai Laporan Projek Sarjana Muda (PSM)

DECLARATION

I admitted that this project title name of

DIGITAL KEY FOR WEB SITE AUTHENTICATION

is written by me and is my own effort and that no part has been plagiarized without citations.

STUDENT : _____ Date : 22 NOV 2006

(MOHD. AFIQ BIN HJ AHMAD)

SUPERVISOR : _____ Date : 22 NOV 2006

(SITI RAHAYU BT SELAMAT)

DEDICATION

To my beloved parents, Hj Ahmad Bin Hj Seman and Mahani Binti Bakar

To my sister, Noor Haniem Bt Hj Ahmad, my brothers Mohamad Sahal Bin Hj Ahmad and Mohamad Nabil Bin Hj Ahmad.

To Noramiza bt Abdullah and all my friends for this steadfast support.

ACKNOWLEDGEMENT

In the name of Allah the Almighty and most Merciful

Firstly, I would like to express my gratitude to Mrs. Siti Rahayu Bt Selamat and Mrs. Aslinda Bt Hassan, my faculty supervisors for facilitating me in the process of undergoing my Projek Sarjana Muda I (PSM I) and Projek Sarjana Muda II (PSM II). I would also like to thank all my lecturers for aiding me with strong academical and technical knowledge that successfully implemented during PSM I and PSM II besides giving motivation to gain self-belief and confidence in the process of developing the project.

I would also like to thank my family for giving me endless support and encouragement throughout my project.

Last but not least, I would like to convey my special thanks to all of my course mates for giving me endless cooperation through thick and thin.

ABSTRACT

Web site Authentication Using Digital Key is a project that focuses the authentication of web site using digital key. The main objective of this project is to authenticate user that surf the web site and to authorize user for what they want to do or access. This project is to develop a system that can exceed the Internet access vulnerabilities. A research is made on current system and on other several thesis to find an information that can help in developing the system. A System Development Life Cycle (SDLC) is select a project reference process flow and to make sure implementation of system running in sequence. From the analysis, the project implementation are using Java Script Programming Language and the RSA(Rivest-Shamir-Adleman) for the cryptography algorithm. In summary, Web Authentication Using Digital Key is a system where its function is to help in internet security and to resolve problem occur in current internet surfing problem.

ABSTRAK

Projek ini menfokuskan tentang pengesahan sesebuah laman web dengan menggunakan kunci digital. Objektif utama projek ini adalah untuk mengesahkan dan memberi hak kebenaran kepada pengguna apakah yang ingin diakses oleh pengguna semasa melayari laman web. Projek ini bertujuan untuk membangunkan sebuah sistem yang boleh menghalang pencerobohan semasa mengakses internet. Penyelidikan telah dilakukan terhadap sistem yang sedang diguna pakai dan seterusnya adalah dengan mencari lebihan maklumat yang dapat membantu untuk membangunkan sistem ini kelak. SDLC (Sistem Development Life Cycle) dipilih sebagai rujukan untuk proses aliran dan untuk memastikan pembangunan sistem dijalankan mengikut turutan. Daripada analisis yang dibuat, projek yang akan dibangunkan menggunakan Bahasa Java Script Programming dan RSA(Rivest-Shamir-Adleman) untuk algoritma kriptografi. Sebagai rumusan , projek ini berfungsi dengan membantu keselamatan internet dan mengatasi masalah yang berlaku semasa melayari laman web.

LIST OF TABLES

LIST OF FIGURES

LIST OF ATTACHMENTS

CHAPTER I

INTRODUCTION

1.1 Overview

Digital keys bind a cryptographic key with one or more attributes of a user. Issued by key authorities, the keys protect the Internet by assuring the authenticity of network messages. This technology and its underlying digital signatures are now helping fuel the deployment of electronic commerce on the Internet. Internet users, developers, administrators, and corporate buyers need to have a solid understanding of certificate-based security systems in order to harness their potential.

1.2 Problem Statement

The Keys to secure Web sites Project that will implement is optional whether for industry or an organization. Nowdays realtime/on demand digital key are very popular either at industry or organization. The problems identified are:

i) Non-Secure Website

From observation, some of company, industry or organization never implement a digital key to access applications on their websites. For this project, digital key can secure the sites that require a very high level of trust between the consumer and the company that is offering its services on the Web. In order for people to trust the company that they are dealing with, they must know that the information they exchange will remain private, and they must be assured of the company's identity [1].

ii) Inconvenient of key algorithm

To realize the digital key,type of algorithm that use are important to suitable and make an improvement for the sites.Each algorithm have an advantages and also have a weaknesses, so looked an enormous advantage for the algorithm that can use is very important. [2]

1.3 Objective

The objectives for this project are :

i. To develop system that provides a digital key.
ii. To authenticate user that surf the web site.
iii. To authorize user for what they want to do or access.

1.4 Scope

The scope of this project are to develop a system that can exceed the Internet access vulnerabilities. There are:

i. Websites visited and its contents.
ii. Digital key to provide authentication to sites.

This digital key need to implement into web site that also need to develop by using Java Programming.

1.5 Contributions

Many enterprises have deployed a Public Key Infrastructure (PKI) for a digital key in order to use digital certificates to address their organization's security needs [3]. While digital certificates are an excellent way to help establish the identities of parties wishing to communicate securely or engage in electronic transactions, like any other credentials, digital certificates can be trusted only if they are shown to be valid at the time they are presented. The world abounds with examples where trust in a credential is achieved only after its validity is established. Drivers' licenses and passports are obvious examples of credentials that are routinely verified when presented.

1.6 Expected Output

Digital Key System consist a form that need user to fullfill for become a key/certificate that allow user to access an application.In this case,user will input the information that require and system will generate the random private key for the user as look as figure below:

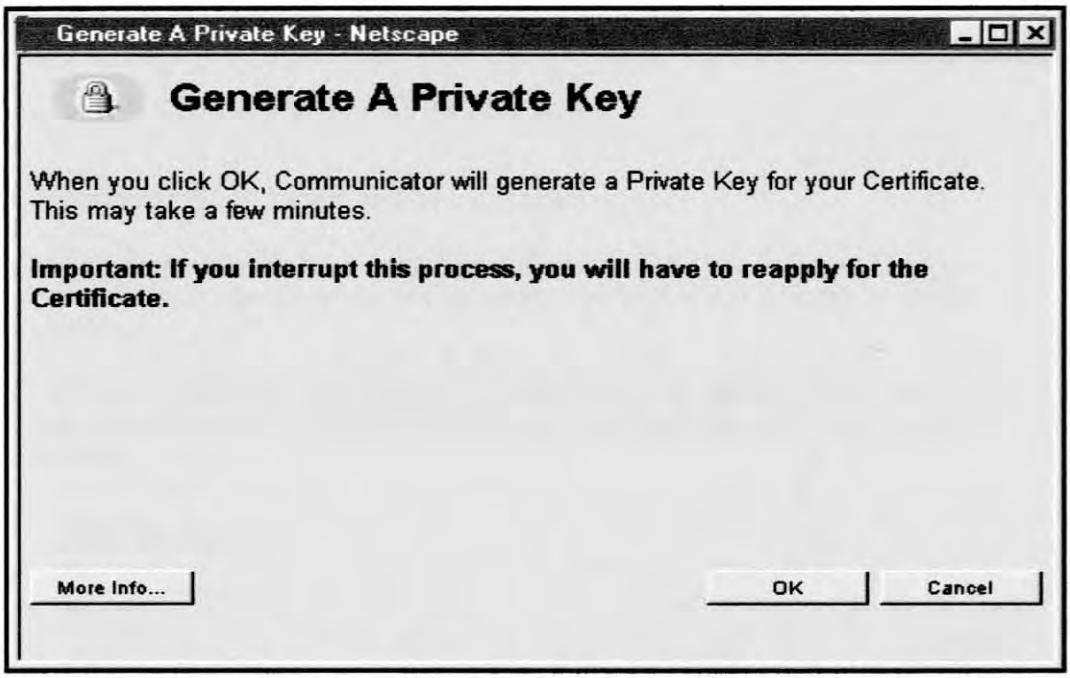

Figure 1.1 : Initial interface for generate private key

Figure 1.2 : User Certificate Name

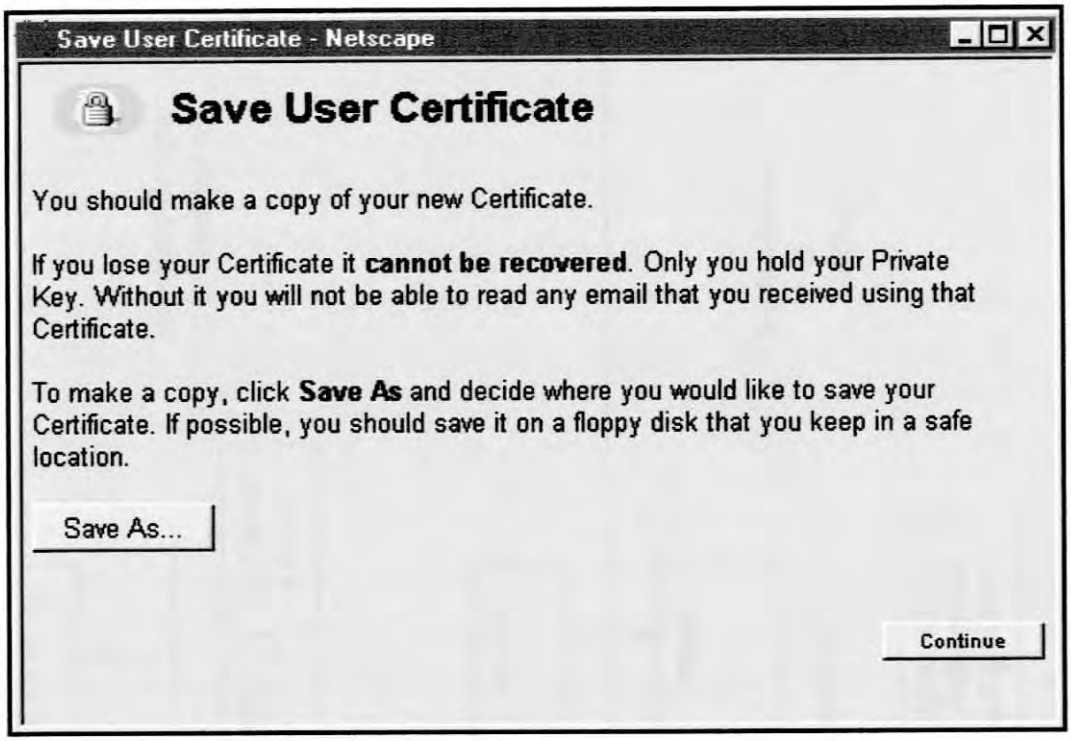

Figure 1.3 : Interface for user certificate copy

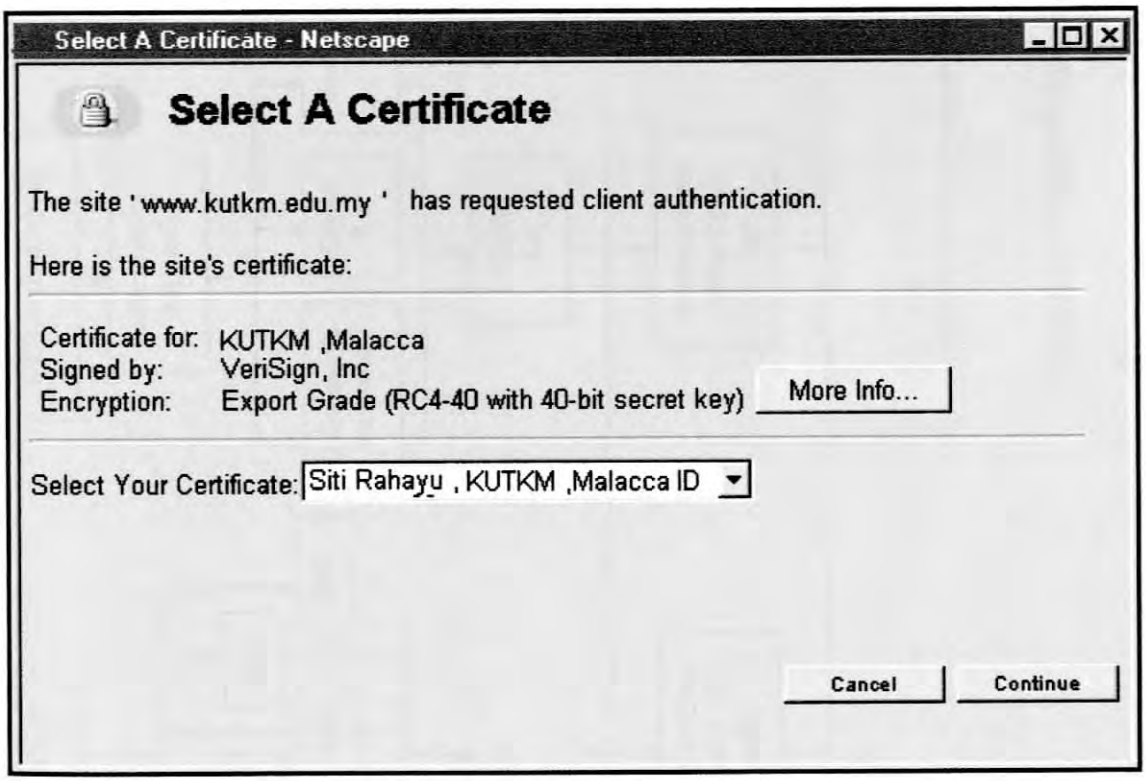

Figure 1.4 : Selection certificate interface

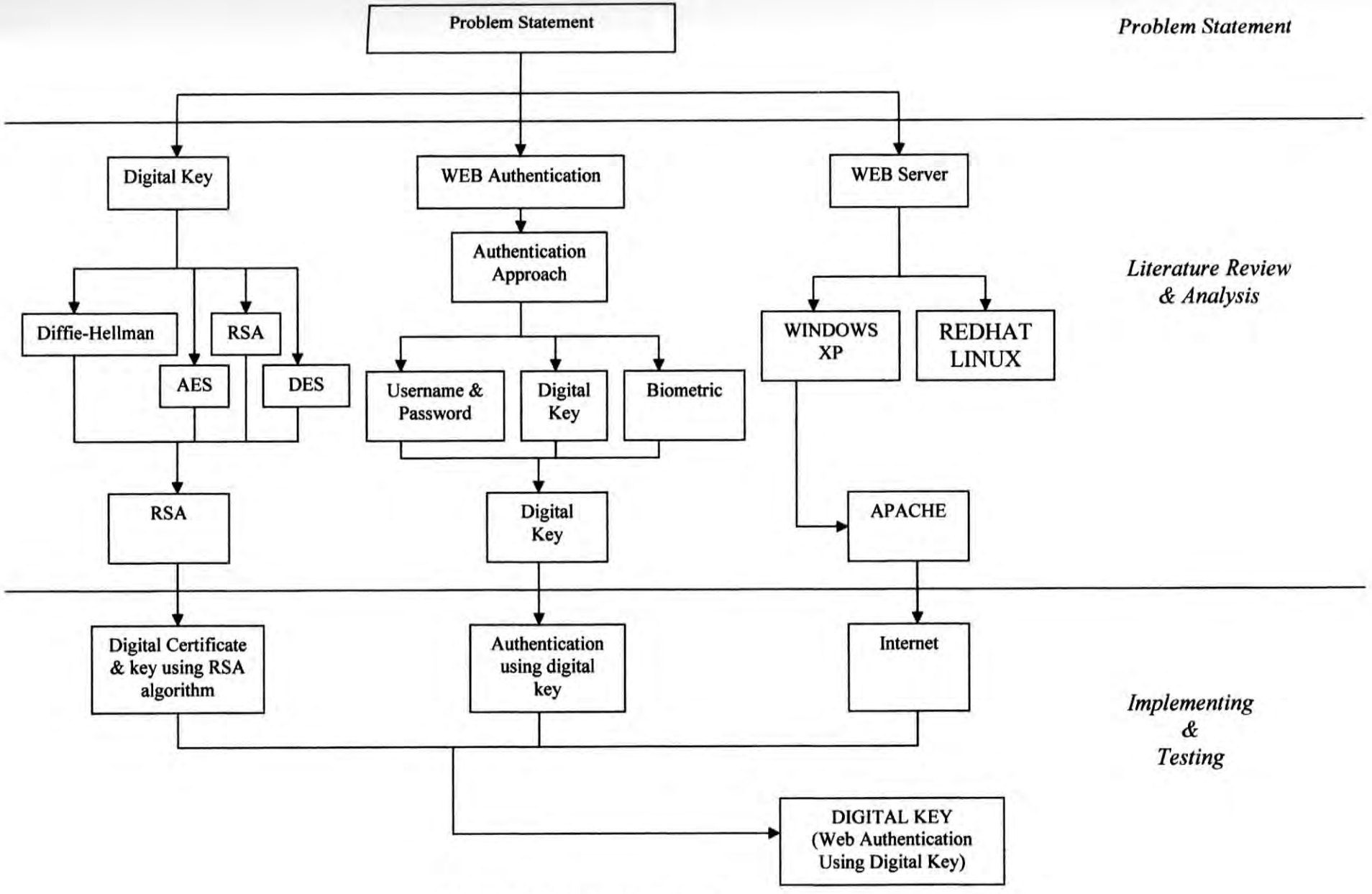

Figure 1.5: Project framework

1.8 Conclusion

Digital key in the digital certificates are an excellent way to help establish the identities of parties wishing to communicate securely or engage in electronic transactions, like any other credentials, digital certificates can be trusted only if they are shown to be valid at the time they are presented.

The Internet has opened up new ways for organizations to communicate, both internally and externally. Better communication between employees, vendors, and customers enables an organization to cut costs, bring products to market faster, and build stronger customer relationships. This improved communication requires at times transmitting sensitive information over the Internet and intranets. It thus becomes imperative to be able to conduct private, tamper-proof communication with known parties. To bring this about, organizations can build a secure infrastructure based on public-key cryptography by using digital certificates. Digital certificate validation is the security hole of many of the key's now being put in place to protect parties engaging in secure application. Without a reliable way of checking the validity of every digital certificate presented to an application, the relying parties in a transaction have no legal recourse should someone use a certificate in some rogue or malicious fashion.

CHAPTER II

LITERATURE RIVIEW AND PROJECT METHODOLOGY

2.1 Introduction

Literature review and project methodology is the main and important things for this Digital Key Project to make sure the project run smoothly. For this project literature review, there are four basic security services is a key point: integrity, confidentiality, identification and authentication, and non-repudiation. This section describes the four services and why they may be necessary in a particular application.

i. ***Data integrity*** services address the unauthorized or accidental modification of data. This includes data insertion, deletion, and modification. To ensure data integrity, a system must be able to detect *unauthorized* data modification. The goal is for the receiver of the data to verify that the data has not been altered.

ii. ***Confidentiality*** services restrict access to the content of sensitive data to only those individuals who are authorized to view the data. Confidentiality measures prevent the *unauthorized* disclosure of information to unauthorized individuals or processes.

iii. ***Identification and authentication*** services establish the validity of a transmission, message, and its originator. The goal is for the receiver of the data to determine its origin.

iv. ***Non-repudiation*** services prevent an individual from denying that previous actions had been performed. The goal is to ensure that the recipient of the data is assured of the sender's identity.

2.2 Fact and Findings

2.2.1 Digital Key Concepts

Communicate with electronically is harder to prove an identity and verify someone else's. For some people, this is not very important, but if someone are finalizing a very profitable business deal over e-mail, for example, definitely want to recognize who is he dealing with whether the person communicating with him is really the right person. Digital key with certificate called Digital Certificate represent a solution to this problem.

Digital certificates are a collection of information about an entity (an individual or corporation) that is certified by an independent agency. They are the electronic equivalent of a driver's license, a credit card, or other identity card. With the right software, a digital certificate can be used to generate digital signatures, which would correspond for own written signature. Therefore, digital certificates provide a signature that is compatible with electronic business.

2.2.2 Web Authentication Concept

Resources are allocated to users. User ID (UID) is a number that identifies the owner of resources:

i. File-owner UID:

The person who originally created the file and processes create files. So file assumes the identity of the process owner UID

ii. Process-owner UID:

User that spawned the process, all processes owned by the same user are spawned indirectly by the initial login process that authenticated the user and child processes inherit ownership from parents

iii. Authentication

User indicates the account by typing the account name. The system then associates the UID with that name. UID indicates account name belongs to Rick. The account name is not secret. So anyone can access the a/c name simply by knowing the name. The solution is each a/c name has a secret password associated with it and only the user knows the password. User is challenged to write in the secret word. Make it difficult to guess.

2.2.3 Cryptography Algorithm Concept

Digital Certificate is a public key certificate that contains a public key intended for verifying digital key and certificate rather than encrypting data or performing any other cryptographic functions. The cryptography algorithm such as RSA, PGP, and PKI is a public key cryptography and DES and AES is a modern secret key cryptography.

Cryptography is a branch of applied mathematics concerned with transformations of data for security. In cryptography, a sender transforms unprotected information (plaintext) into coded text (cipher text). A receiver uses cryptography to either:

i. Transform the ciphertext back into plaintext
ii. Verify the sender's identity
iii. Verify the data's integrity or some combination.

In many cases, the sender and receiver will use *keys* as an additional input to the cryptographic algorithm. With some algorithms, it is critical that the keys remain a secret. If Charlie is able to obtain secret keys, he can pretend to be Alice or Bob, or read their private messages. One of the principal problems associated with cryptography is getting secret keys to authorized users without disclosing them to an attacker. This is known as secret key distribution. This document will examine three commonly used classes of cryptographic mechanisms that are symmetric algorithms, secure hash algorithms, and asymmetric algorithms. For each class, need to discuss which of the four security services can be supported. In addition, we will discuss whether the algorithm can be used for secret key distribution.

2.2.4 Types of Digital Key Algorithm

The Keys to secure Web sites Project devide for many types such as PKI (Public Key Infrastructur), RSA (Rivest-Shamir-Adleman), AES (Advanced Encryption Standard), DES (Data Encryption Standard) and others:

i) PKI (Public Key Infrastructure)

A public key infrastructure (PKI) is a foundation on which other applications, system, and network security components are built. A PKI is an essential component of an overall security strategy that must work in concert with other security mechanisms, business practices, and risk management efforts. PKI is a broad subject matter and is constantly evolving to meet the growing demands of the business world. This article