iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** VI **Month of publication:** June 2019

DOI: http://doi.org/10.22214/ijraset.2019.6242

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue VI, June 2019- Available at www.ijraset.com

A Vital Role of Digital Certificate in E-Commerce Security

Prashant P. Pittalia
Department of Computer Science, Sardar Patel University

Abstract: ***It necessity for any kind of business to use the internet technology to allows organization to enhance their critical operation, attract the new markets, and enhancement of services for customers as well as for providers. E-commerce is very important tool in such organization with properly implementation of security. People are diverted to doing their work online like money transaction, pay online, exchange credential information etc. Through E-commerce the organization may do the business world wide with the help of internet. The major problem with the e-commerce sites are security and privacy. Privacy means that the credential information of the users should be kept secure. Security means that unauthorized users are not allowed to access any resources of the website. E-commerce security is the protection of e-commerce assets from unauthorized access, destruction or alteration.To provides the security of E-commerce transaction organization must need a digital certificate from the authorized certificate authority. Digital certificates are working on the public key and private key concept of the asymmetric key algorithms. The purpose of this paper is to explain the types of digital certificate, fields used in digital certificate and how it helps into provide E-commerce security.***

Keywords: Public key cryptography, digital certificate, E-commerce security

I. INTRODUCTION

The rapid development of Internet e-commerce has a new model of business activities. E-commerce on-line transmission the data security must be demanded. E-commerce may include the use of electronic data interchange, electronic money exchange, Internet advertising, websites, online databases, computer networks, and point-of-sale computer systems. E-commerce major concerns on privacy, security and trust.

Both the buyer and seller on e-commerce websites concern about the credential information they are exchanges or stored on the devices at the sometime they insist that intruder is not able to access or misuse the content they are transferring to each other. It is needed to make computer security & data security. The successful functioning of E-commerce security depends on a complex interrelationship between several applications development platforms, database management systems, systems software and network infrastructure [1].

To achieve it the security services like Integrity, Privacy, Non-repudiation, Authenticity, Confidentiality, and Availability must be implemented. Integrity makes sure that during transmission the data was not tampered. Authentication proves the identity of the user. Confidentiality provides the secrecy of the message so intermediate users are not able to read or understand the message transmit between the actual sender and the receiver.

Availability means that resources should be available 24*7 to the users. Non-repudiation means if any discrepancy between sender and receiver is created that to identify the truth in it. In e-commerce it is need to take care of the serious problem like unauthorized user is access the resource as well as tampering the data or information. Gaining access to sensitive information and replay are some common threats that hackers impose to E-commerce systems [2]. Digital certificate is very useful to ensure the integrity and non-repudiation of transaction on e-commerce website. Digital certificates provide for confirming identities in E-commerce websites. It is used in public and private sectors.

II. DIGITAL CERTIFICATE

In cryptography, digital certificate or identity certificate is also known as a public key certificate, is an electronic document used to prove the ownership of a public key. Digital certificate includes public key and private key, information about the identity of its owner known as subject and the digital signature of an entity that has verified the certificate's contents known as issuer. If the signature is valid, and the software examining the certificate trusts the issuer, then it can use public key to communicate securely with the certificate's subject. In a certificate's subject is typically a person or organization. However, in Transport Layer Security (TLS) a certificate's subject is a computer or device. HTTPS (Secure Hypertext Transfer Protocol) protocol is used to show that the website is trustworthy. Certificate authority (CA) usually a company that issue the certificate to a customers on chargeable basis

under public-key Infrastructure (PKI) scheme. When you conduct business online whether it's selling products through a Web site or simply using email for company communication the business is not face to face.

To address this risk, digital certificates were created. If you use the Web to transact business or communicate sensitive information with clients, then digital certificates are a must. In a public key environment, it is critical that you are assured that the public key to which you are encrypting data is in fact the public key of the intended recipient and not a fake. You could simply encrypt only to those keys, which have been physically handed to you.

But suppose you need to exchange information with people you have never met; how can you tell that you have the correct key? Digital certificates, simplify the task of establishing whether a public key truly belongs to the purported owner. A certificate is a form of credential. Examples might be your driving license, your passport, or your birth certificate. Each of these has some information on it identifying you and some authorization stating that someone else has confirmed your identity. Some certificates, such as your passport, are important enough confirmation of your identity that you would not want to lose them, in case someone uses them to impersonate you.

A digital certificate is data that functions much like a physical certificate. A digital certificate is information included with a person's public key that helps others verify that a key is genuine or valid. Digital certificates are used to prevent attempts to substitute one person's key for another.

The contents of certificates are organized according to the X.509 v3 certificate specification, which has been recommended by the International Telecommunications Union (ITU), an international standards body, since 1988. An X.509 certificate is a collection of a standard set of fields containing information about a user or device and their corresponding public key. The X.509 standard defines what information goes into the certificate, and describes how to encode it. Certificate Authority: Digital certificates are generated and themselves digitally signed by organizations known as certificate authorities. It is the job of a certificate authority to verify the identity of the person requesting a digital certificate before issuing one to them.

III.DIGITAL CERTIFICATE TYPES

A. Personal Certificates

These certificates identify individuals. They may be used to authenticate users with a server, or to enable secure e-mail using S-MIME. A personal digital certificate is like a digital ID card, which Company or University uses to verify employee identification before granting his/her access to certain protected resources. Because certificates may be installed differently depending on the application employee are using, employee may have multiple certificates on their system. CA's Digital IDs for Secure Email allow you to digitally sign and encrypt your digital communications using a Digital ID, bound to your validated email address. Recipients of your email will know that the content came from your email address and has remained private during transmission.

B. Server Certificates

Server certificates identify servers that participate in secure communications with other computers using communication protocols such as SSL. These certificates allow a server to verify its identity to clients. Server certificates follow the X.509 certificate format that is defined by the Public-Key Cryptography Standards (PKCS).

C. Software Publisher Certificates

These certificates are used to sign software to be distributed over the Internet. It just informs the user that the publisher is trusted or not. It could not give the guarantee that signed code is safe to run. Internet Explorer is also capable of trusting software that is signed with a publisher's certificate. To view a list of trusted software publishers in Internet Explorer, click Internet Options on the Tools menu, click the Content tab, and then click Publishers. You can also remove trusted publishers by clicking Remove in this screen.

D. Certificate Authority Certificates

Internet Explorer divides CAs into two categories, Root Certification Authorities and Intermediate Certification Authorities. Root certificates are self-signed, meaning that the subject of the certificate is also the signer of the certificate. Root Certification Authorities have the ability to assign certificates for Intermediate Certification Authorities. An Intermediate Certification Authority has the ability to issue server certificates, personal certificates, and publisher certificates, or certificates for other intermediate certification authorities.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue VI, June 2019- Available at www.ijraset.com

IV. STRUCTURE OF DIGITAL CERTIFICATE

The X.509, PKI X.509 and Public Key Cryptography Standards (PKCS) defines the standard formats for digital certificates and their use. Public Key Infrastructure (PKI) is consists of protocols, standards and services to authenticate users using digital certificates that are issued by CA. A digital certificate structured in a standard way so that information within the certificate can be retrieved and understood regardless of who issued the certificate. Digital certificates contains various fields.

1) *Version:* It indicates the version of digital certificate. There are three version exist for digital certificates.
2) *Serial Number:* When the certificate authority issues a digital certificate to any client it provides a unique identifier for each certificate.
3) *Signature Algorithm ID:* It is the asymmetric key algorithm (Public Key Algorithm) used by the certificate authority to sign the client certificates.
4) *Issuer Name:* Provides a distinguished name for the CA that issued the certificate. The issuer name is commonly represented by using an X.500 or LDAP format. For a root CA, the Issuer and Subject are identical. For all other CA certificates and for end entity certificates, the Subject and Issuer will be different.
5) *Validity Period:* It shows the period of time for which the certificate is valid. It provides the date and time when the certificate becomes valid and when the certificate is no longer considered valid.
6) *Subject:* The owner identity. It is the name of the computer, user, network device, or service. The subject name is commonly represented by using an X.500 or Lightweight Directory Access Protocol (LDAP) format.
7) *Subject Public Key Info:* It contains the public key of the owner of the certificate and the public key algorithms associated with the public key.
8) *Issuer Unique ID:* It is the id to uniquely identify the issuer of the certificate.
9) *Subject Unique ID:* It is the id to uniquely identify the owner of the certificate.
10) *CA Digital Signature:* It contains the actual digital signature of the CA.
11) *Extension:* In addition to the fields defined in X.509 version 1, X.509 version 3 certificates include optional fields or extensions that provide additional functionality and features to the certificate. These extensions are not necessarily included in each certificate that a CA issues. Extension are Subject alternative name, Basic constraints, Name constraints, Policies, Policy mapping, Policy constraints, Application policy, Application policy mapping, Cross certificate distribution points, CRL distribution points (CDP), Authority Information Access (AIA), Enhanced Key Usage (EKU) [5].

The structure of an X.509 digital certificate is as shown in below figure.

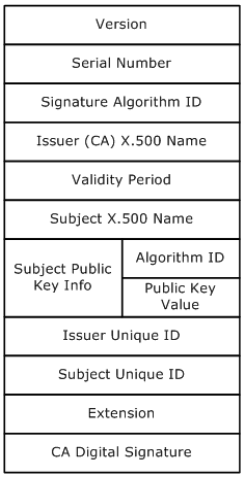


Fig. 1 Digital Certificate Format [3]

When we visit any website on Internet, if we wants to identify that the website is secure or not, we have to check the URL (Uniform Resource Locator) starts with https (Secure Hypertext Transfer Protocol). It means that the website having a valid digital certificate and if we do any operations on such websites it is safe. To see the digital certificate of a particular website we have to click on the pad lock display on left side of URL. For example if we you wants the certificate details of amazon website then in your web browser address bar type https://www.amazon.com and click on the padlock shown in the left side of address bar. After that click on Certificate (Valid) link over there, it should look like as below figure.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue VI, June 2019- Available at www.ijraset.com

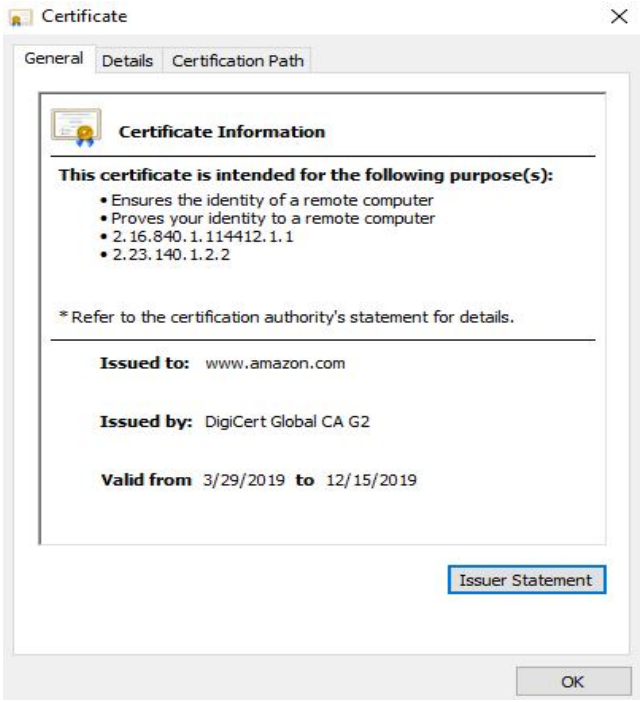


Fig. 2 Digital Certificate of Amazon Website [4]

When you click on the detail tab option on digital certificate it will show all the parameters regarding it as shown below.

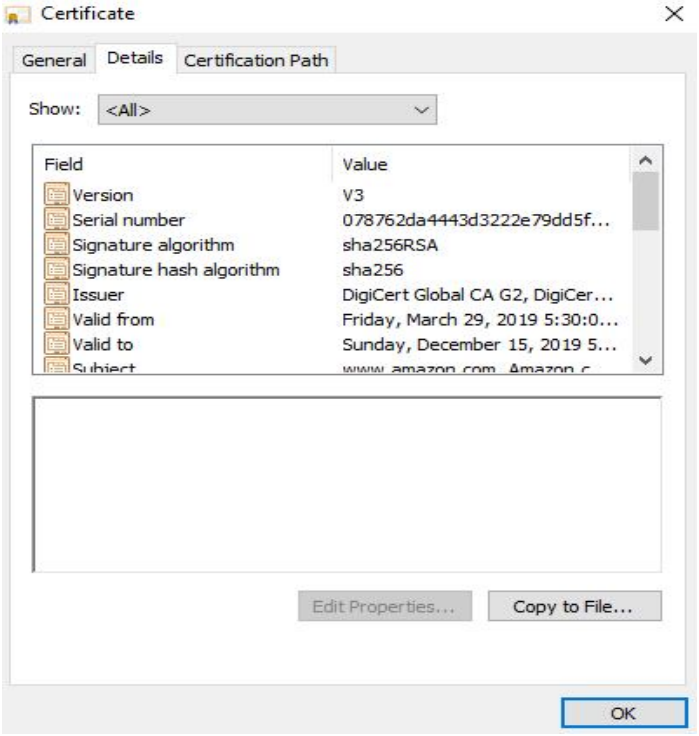


Fig. 3 Digital Certificate of Amazon Website [4]

Same way when you click on the certification path tab option on digital certificate it will show who the owner of this digital certificate is. Also it shows the hierarchy of the certificate authority from current to root certificate authority. In this example it shows that the DigiCert Global CA G2 is certificate authority who issue the certificate to the amazon.com owner. Also the root certificate authority is Verisign.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue VI, June 2019- Available at www.ijraset.com

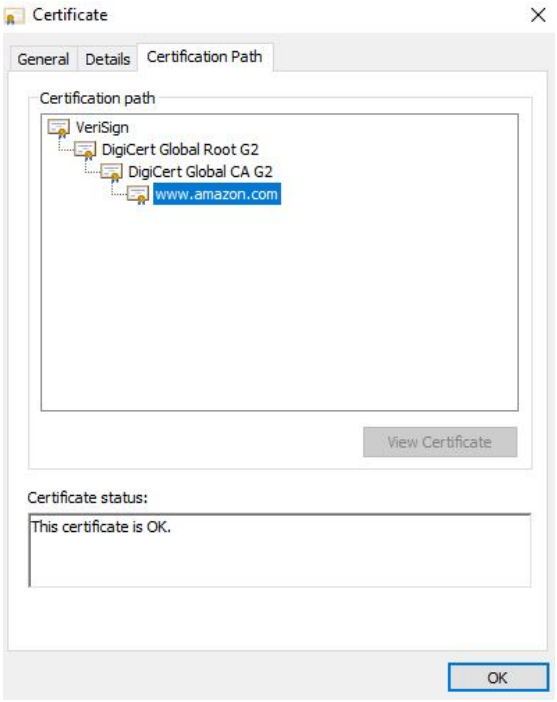


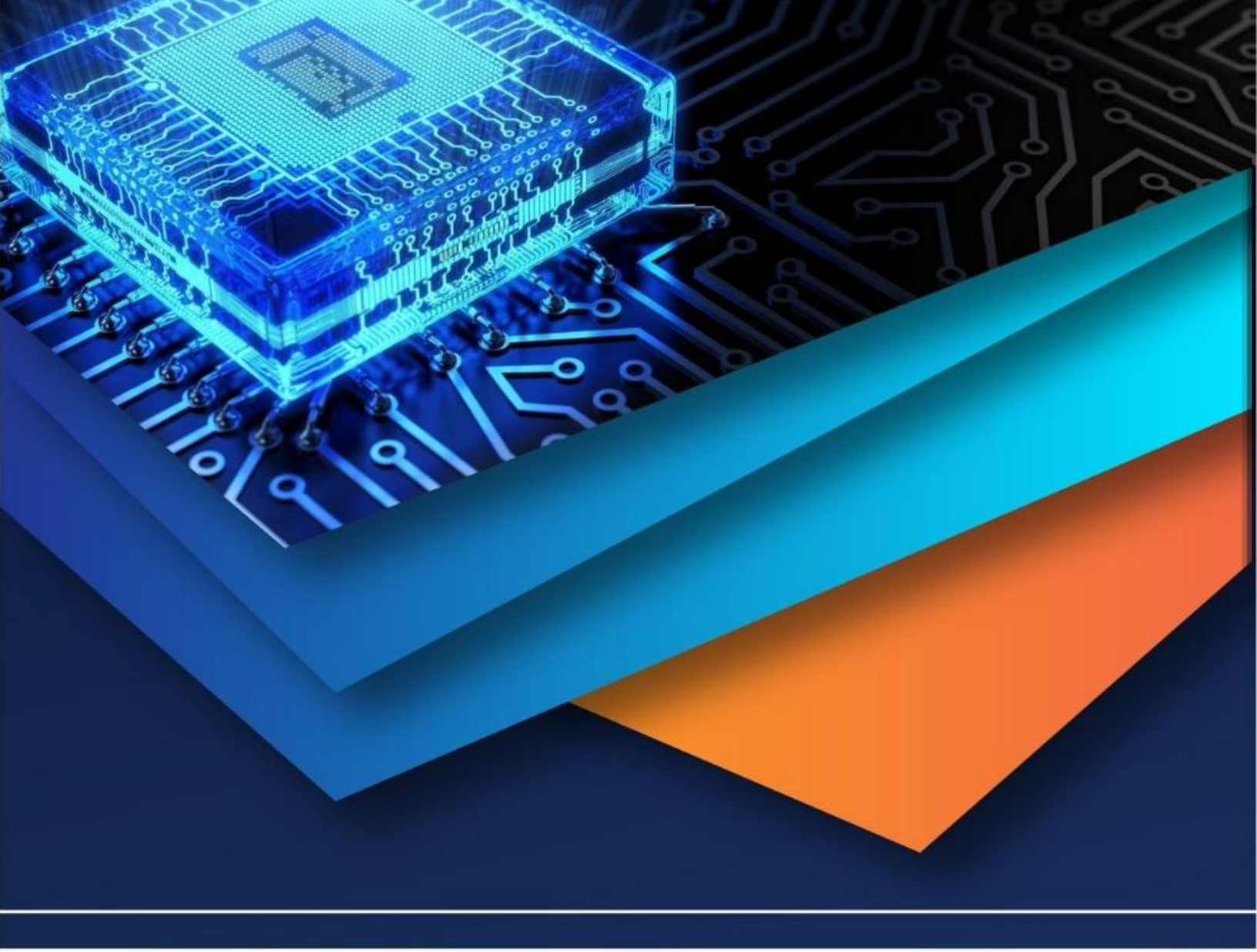
Fig. 4 Digital Certificate of Amazon Website [4]

V. CONCLUSIONS

E-commerce is now a part of every business at the same time it is very important to protect the information exchanges and storing on devices. Intruders easily identify the weaknesses in the websites by utilizing some malicious programs or software's. To protect against various passive and active attacks of intruders and make the trustworthy website for the end-users, it must to purchase and use the digital certificate as per the requirement of the individuals or organization in private and public sector.

REFERENCES

[1] S. R. S. KESH, AND S. NERUR, "A Framework for Analyzing E-Commerce Security," Information Management and Computer Security, vol. 10, no. 4, no. pp. 149-158.
[2] D. Berlin, "Information Security Perspective on Intranet," presented at Internet and E-Commerce Infrastructure, 2007.
[3] https://sites.google.com/site/amitsciscozone/home/security/digital-certificates-explained
[4] https://www.amazon.com/
[5] https://knowledge.digicert.com/solution/SO4583.html



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY