<https://www.makeuseof.com/tag/encrypted-email-android-openkeychain/>

<https://www.youtube.com/watch?v=Z0WlQOvn3RA>

<https://www.youtube.com/watch?v=tmeHBM1cAgs>

hashing, Digital Signature and Digital Certificates

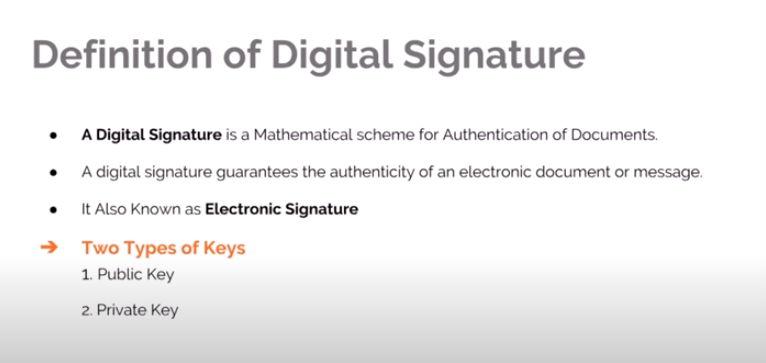
<https://www.geeksforgeeks.org/digital-signatures-certificates/#:~:text=Digital%20signature%20is%20like%20a,holder's%20identity%20and%20provides%20security.&text=Hashed%20value%20of%20original%20message,to%20generate%20the%20digital%20signature>

Digital Signature:

Understanding the Differences

The primary difference between the digital signature and the digital certificate:

1. The certificate ties the *digital signature* to a data object, while the *digital signature* secures the data in transit.
2. The *digital certificate* uses the public key to identify the data's source, while the *digital signature* uses the public key to verify the data's integrity.



PGP:

<https://digitalguardian.com/blog/what-pgp-encryption-defining-and-outlining-uses-pgp-encryption>

<https://www.tutorialspoint.com/network_security/network_security_application_layer.htm>

SSL:

<https://www.digicert.com/ssl-cryptography.htm>

SSL: Secure Sockets Layer.

## What is the SSL certificate in e-commerce?

In present-day era the acronym SSL has expand its demand in market environments,The SSL certificate in e-commerce acknowledge to the [symbol](https://www.wordhippo.com/what-is/another-word-for/symbol.html)s Secure Sockets Layer.It is a web protocol which is originate to allow huge security in insecure online communications. This certificate come up with a secure channel or secure medium between two devices (end points devices such server,mobile phones, computers,laptop etc. during data exchange or data transnfer.In Todays ,world it is use in most of transaction as well as **most communications, take place in internet environments.** This assits to know why modern criminals have made most of the activity using internet.

Malware, phishing, vishing, DoS attacks, credit/debit card fraud and a host of other threats put the security of e-commerce stores at risk.here SSL play a most important role .Their purpose is simple: first of all, **they encrypt and safeguard data transferred between browsers and servers**Another thing SSL always provide **authenticate the server to which the device is connecting**. The motive of this activity is to protect online consumers.

Thirdly, **these certificates analyze and verify the data sent**, in order to prevent malware and other threats from affecting any of the two parties involved in the communication (server and mobile device, for example).

## Reason of using SSL Certfifcate:

### fringe benefit to the comprehensive security of e-commerce

without [SSL certificates](https://www.ecommerce-nation.com/ssl-set-and-other-ecommerce-security-protocols/" \t "_blank) in online transaction,bank and in e-commerce will definitely place at threat the defence of confidential information such as user names, passwords, credit card information, etc.

Although not all cybersecurity in these domain hang on on SSL these certificate can be used as a backups for instance HTTPS protocols or PCI DSS standards somehow include security mechanism , having this certificate brings added value.

### strengthen End-user trust:

Usually,almost all e-commerce store has an SSL certificate, because sometime online consumers also find out and thanks to the green padlock that appears in their browser. They don’t want their password and credit card information to be travel in plain text .

### Most End-Users concern About security in online shopping:

Most of the user concern about SSL certicate while using shopping **SSL certification and other trust seals begin to be included in their purchase decision.**

### protection credit card information

Was it compulsory to bring up this advantage of SSL certificates in e-commerce? Of course not!

But even so, **we will underline that its installation allows adding an extra layer of security to credit and debit card payments.**

If you also try to process these types of payments through online gateways (PayPal, Stripe, etc.), you will multiply your security as a seller and that of your customers.

### Improve search engine positioning

**Google and its algorithms never rest** – they’re always being better and perfected!

In 2019 more than ever, **they will give more importance to the use of HTTPS protocols and SSL certificates.**

.

Reference: <https://www.ecommerce-nation.com/ssl-in-ecommerce/>

**vulnerabilities in SSL**

<https://www.acunetix.com/blog/articles/tls-vulnerabilities-attacks-final-part/>

* SSL and TLS basically used as a security protcols.The Secure Sockets Layer (SSL) and the Transport Layer Security (TLS) are cryptographic protocols have had their allotment of blemish for instance all other automation.
* These protcols have some version like (TLSv1.2 and older) but one major vulnerability was found that affects TLS 1.3.some of the vulnerability is also based on a forced downgrade attack is listed down.

**CRIME**

Crime acroymn of Compression Ratio Info-leak Made Easy (CRIME) is an attack in opposition to TLS/SSL,Crime has a plentiful inappreciable probability of exploitation.

The writer of CRIME and BEAST attack is same. In Crime, basically the attacker essential a man-in-the-middle connection and the ability to frequently introduce unsurprising data whilst keep an eye on the resulting encrypted traffic. This could be obtainable through Cross-site scripting attacks(XSS) one of the most common vulnerability but in crime JavaScript is not vital and an attack can do it with sampling using HTML Injection alone however it would be less efficient.

For CRIME to be possible the client and server must support  coalescence, of the application before encryption. TLS supports DEFLATE which is vulnerable, as is SPDY.

**BEAST**

BEAST acroymn Browser Exploit in opposition to SSL/TLS (BEAST) is active .it is one of the oldest SSL attack as this attack was found to be possible against TLS v1.0 and SSLv3.0 (and below) when a block cipher is in use. successfully an hacker is good to predict the Initialisation Vector utilised as part of the encryption process meaning that if a duplicate figure is obvious in the plaintext then it will be evident in the ciphertext. However, it is of limited use an it is only possible to retrieve small pieces of data, such as session tokens. The attacker must be able to man-in-the-middle a connection and there must be a way of generating additional traffic such as an SOP bypass or a Cross-site Scripting vulnerability. The user must be using an older web browser, as modern browsers protect against this issue. If all of these conditions are met and session tokens are protected against XSS through a mechanisms such as HttpOnly cookies then an attacker may exploit BEAST to gain access to these protected tokens.

Remediation  
Enforce TLS v1.1 and above  
Alternatively you could accept the risk and rely on the protections offered by modern browsers, or alternatively prefer RC4 ciphers to mitigate beast but introduce their own issues.

.

Still the intruder can snuffle the sender’s message (m, H(m)+s) with difference in the MAC (Message Authentication Code) algorithm.

The intruder can extract ‘s’  from the message ‘m’ by performing hashing H(m). The extraction is performed as (H(m)+s-H(m)).

Also, there is a scope to Trudy send a modified message as he knows the secret key. The message is generated as (m’,H(m’)+s).

**Therefore, the MAC algorithm with the given variation contains flaws.**

[*Heartbleed*](https://www.acunetix.com/blog/articles/aftermath-heartbleed-bug/) was a censorious open to attack that was found in the heartbeat extension of the popular OpenSSL library. This extension is used to keep a connection alive as long as both parties are still there. The Heartbleed vulnerability is registered in the NIST NVD database as [CVE-2014-0160](https://nvd.nist.gov/vuln/detail/CVE-2014-0160).

The client sends a heartbeat message to the server with a payload that contains data and the size of the data (and padding). The server must respond with the same heartbeat request, containing the data and the size of data that the client sent.

The Heartbleed vulnerability was based on the fact that if the client sent false data length, the server would respond with the data received by the client and random data from its memory to meet the length requirements specified by the sender.

Leaking unencrypted data from server memory can be disastrous. There have been proof-of-concept exploits of this vulnerability in which the attacker would get the private key of the server. This means that an attacker would be able to decrypt all the traffic to the server. Server memory may contain anything: credentials, sensitive documents, credit card numbers, emails, etc.