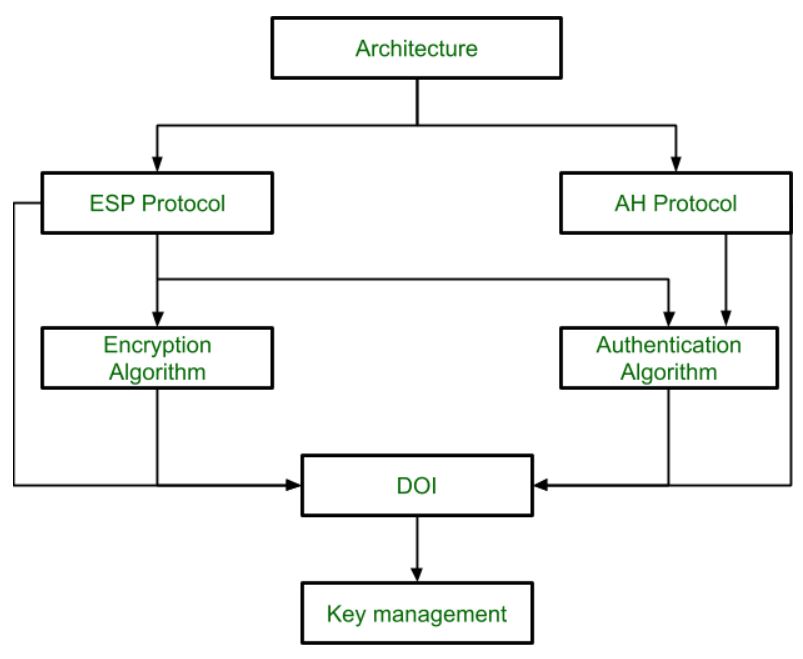
**IPSec Architecture**

**IPSec (IP Security) architecture** uses two protocols to secure the traffic or data flow. These protocols are ESP (Encapsulation Security Payload) and AH (Authentication Header). IPSec Architecture include protocols, algorithms, DOI, and Key Management. All these components are very important in order to provide the three main services: 

* Confidentiality
* Authentication
* Integrity

**IP Security Architecture:**

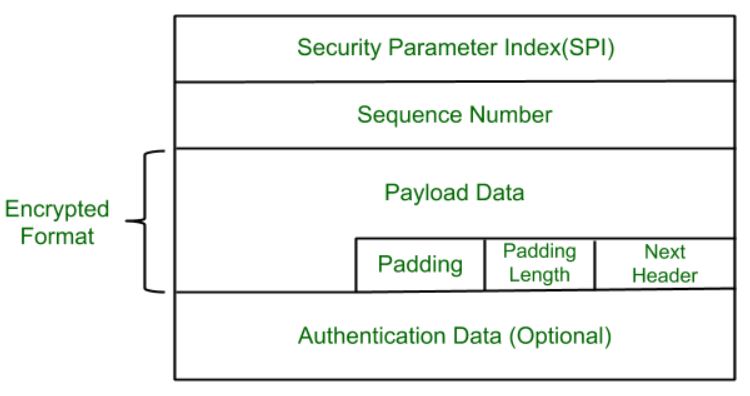


**1. Architecture:**   
Architecture or IP Security Architecture covers the general concepts, definitions, protocols, algorithms and security requirements of IP Security technology.

**2. ESP Protocol:**   
ESP (Encapsulation Security Payload) provide the confidentiality service. Encapsulation Security Payload is implemented in either two ways: 

* ESP with optional Authentication.
* ESP with Authentication.

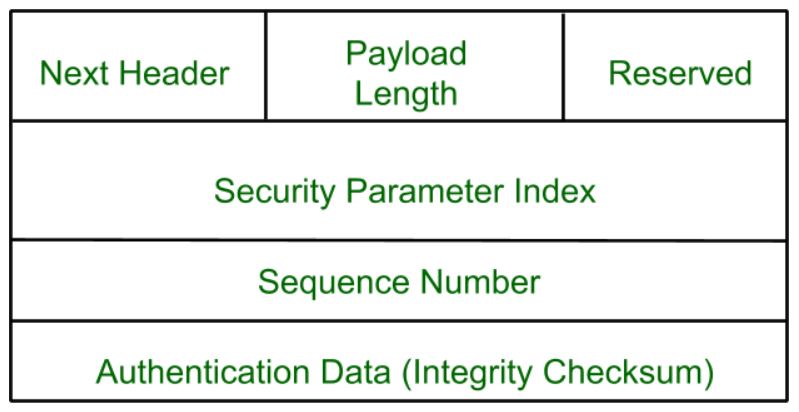
**Packet Format:**



* **Security Parameter Index(SPI):**   
  This parameter is used in Security Association. It is used to give a unique number to the connection build between Client and Server.
* **Sequence Number:**   
  Unique Sequence number are allotted to every packet so that at the receiver side packets can be arranged properly.
* **Payload Data:**   
  Payload data means the actual data or the actual message. The Payload data is in encrypted format to achieve confidentiality.
* **Padding:**   
  Extra bits or space added to the original message in order to ensure confidentiality. Padding length is the size of the added bits or space in the original message.
* **Next Header:**   
  Next header means the next payload or next actual data.
* **Authentication Data**   
  This field is optional in ESP protocol packet format.

**3. Encryption algorithm:**  
Encryption algorithm is the document that describes various encryption algorithm used for Encapsulation Security Payload.

**4. AH Protocol:**   
AH (Authentication Header) Protocol provides both Authentication and Integrity service. Authentication Header is implemented in one way only: Authentication along with Integrity.



Authentication Header covers the packet format and general issue related to the use of AH for packet authentication and integrity.

**5. Authentication Algorithm:**   
Authentication Algorithm contains the set of the documents that describe authentication algorithm used for AH and for the authentication option of ESP.

**6. DOI (Domain of Interpretation):**   
DOI is the identifier which support both AH and ESP protocols. It contains values needed for documentation related to each other.

**7. Key Management:**   
Key Management contains the document that describes how the keys are exchanged between sender and receiver.

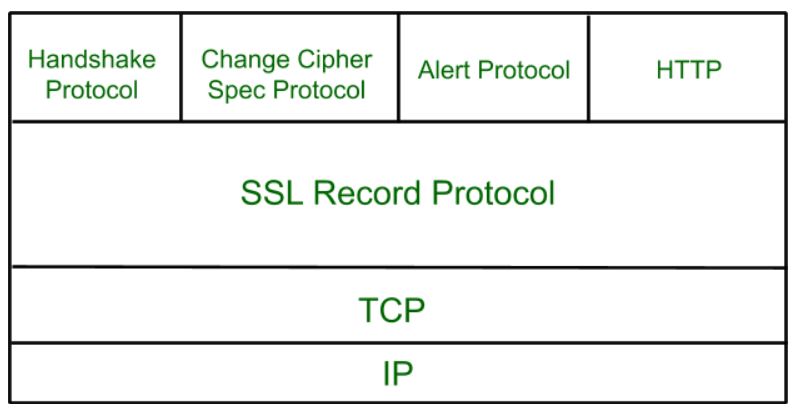
**Secure Socket Layer (SSL)**

Secure Socket Layerprovides security to the data that is transferred between web browser and server. SSL encrypts the link between a web server and a browser which ensures that all data passed between them remain private and free from attack.

**Secure Socket Layer Protocols:**

* SSL record protocol
* Handshake protocol
* Change-cipher spec protocol
* Alert protocol

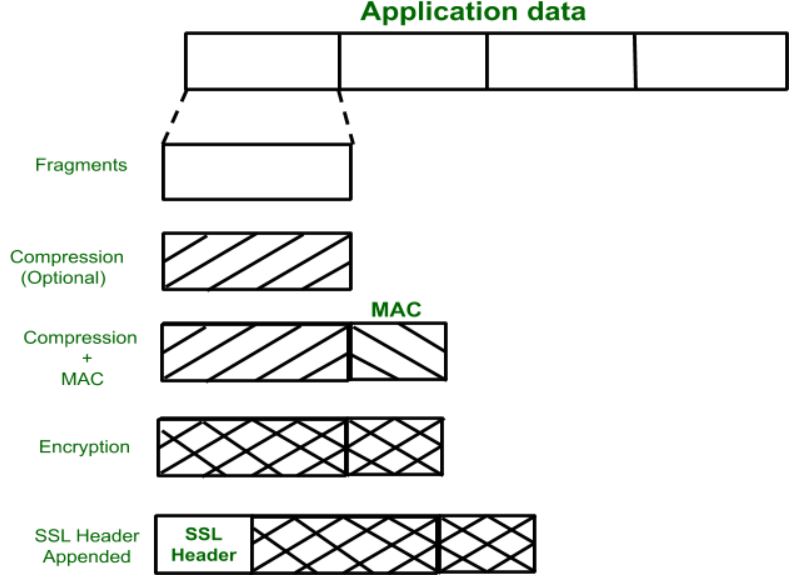
**SSL Protocol Stack:**



**SSL Record Protocol:**   
SSL Record provides two services to SSL connection.

* Confidentiality
* Message Integrity

In the SSL Record Protocol application data is divided into fragments. The fragment is compressed and then encrypted MAC (Message Authentication Code) generated by algorithms like SHA (Secure Hash Protocol) and MD5 (Message Digest) is appended. After that encryption of the data is done and in last SSL header is appended to the data.



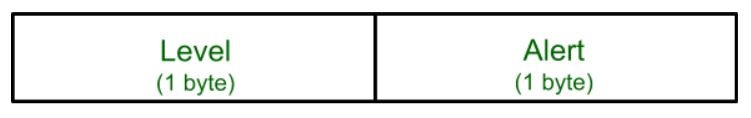
**Handshake Protocol:**   
Handshake Protocol is used to establish sessions. This protocol allows the client and server to authenticate each other by sending a series of messages to each other. Handshake protocol uses four phases to complete its cycle.

* **Phase-1:** In Phase-1 both Client and Server send hello-packets to each other. In this IP session, cipher suite and protocol version are exchanged for security purposes.
* **Phase-2:** Server sends his certificate and Server-key-exchange. The server end phase-2 by sending the Server-hello-end packet.
* **Phase-3:** In this phase Client reply to the server by sending his certificate and Client-exchange-key.
* **Phase-4:** In Phase-4 Change-cipher suite occurred and after this Handshake Protocol ends.

**Change-cipher Protocol:**  
This protocol uses the SSL record protocol. Unless Handshake Protocol is completed, the SSL record Output will be in a pending state. After handshake protocol, the Pending state is converted into the current state.   
Change-cipher protocol consists of a single message which is 1 byte in length and can have only one value. This protocol’s purpose is to cause the pending state to be copied into the current state.



**Alert Protocol:**   
This protocol is used to convey SSL-related alerts to the peer entity. Each message in this protocol contain 2 bytes.

The level is further classified into two parts:

* **Warning:**
  + This Alert has no impact on the connection between sender and receiver.
* **Fatal Error:**
  + This Alert breaks the connection between sender and receiver.

**Silent Features of Secure Socket Layer:**

* The advantage of this approach is that the service can be tailored to the specific needs of the given application.
* Secure Socket Layer was originated by Netscape.
* SSL is designed to make use of TCP to provide reliable end-to-end secure service.
* This is a two-layered protocol.

# Secure Electronic Transaction (SET) Protocol

**Secure Electronic Transaction** or SET is a system that ensures the security and integrity of electronic transactions done using credit cards in a scenario. SET is not some system that enables payment but it is a security protocol applied to those payments. It uses different encryption and hashing techniques to secure payments over the internet done through credit cards. The SET protocol was supported in development by major organizations like Visa, Mastercard, Microsoft which provided its Secure Transaction Technology (STT), and Netscape which provided the technology of Secure Socket Layer (SSL).

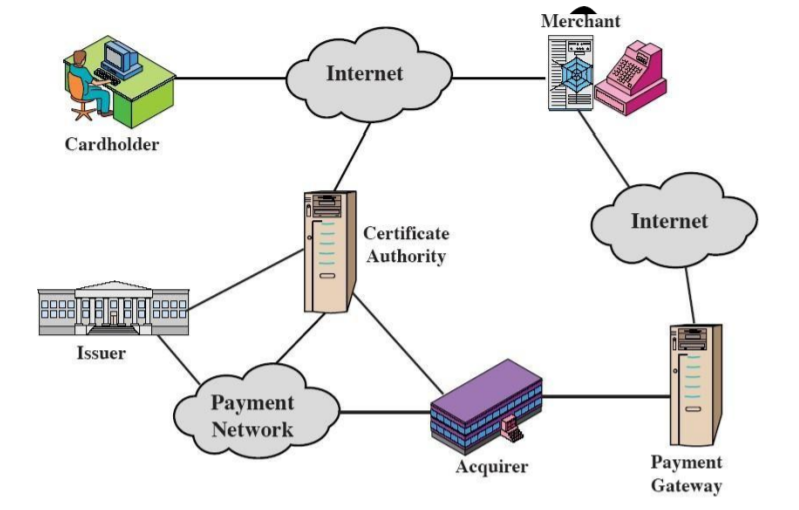
SET protocol restricts the revealing of credit card details to merchants thus keeping hackers and thieves at bay. The SET protocol includes Certification Authorities for making use of standard Digital Certificates like X.509 Certificate.

**SET Participants**

* **Cardholder:** purchasers interact with merchants from personal computers over the Internet
* **Merchant:** a person or organization that has goods or services to sell to the cardholder
* **Issuer:** a financial institution, such as a bank, that provides the cardholder with the 123 payment card.
* **Acquirer:** a financial institution that establishes an account with a merchant and processes payment card authorizations and payments
* **Payment gateway:** a function operated by the acquirer or a designated third party that processes merchant payment messages
* **Certification authority (CA):** an entity that is trusted to issue X.509v3 public-key certificates for cardholders, merchants, and payment gateways

**Events in a transaction**

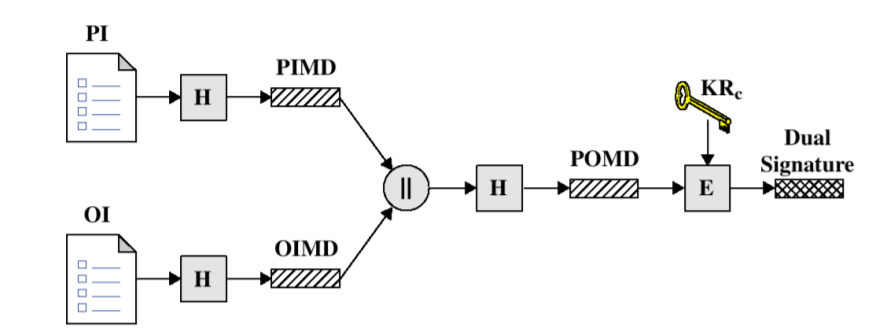
1. The customer obtains a credit card account with a bank that supports electronic payment and SET
2. The customer receives a X.509v3 digital certificate signed by the bank.
3. Merchants have their own certificates
4. The customer places an order
5. The merchant sends a copy of its certificate so that the customer can verify that it's a valid store
6. The order and payment are sent
7. The merchant requests payment authorization
8. The merchant confirms the order
9. The merchant ships the goods or provides the service to the customer
10. The merchant requests payment



* SET also needs to provide interoperability and make use of the best security mechanisms.
* SET Functionalities :
  + Provide Authentication
  + Provide Message Confidentiality
  + Provide Message Integrity

**Dual Signature :**

* The dual signature is a concept introduced with SET
* The customer wants to send the order information (OI) to the merchant and the payment information (PI) to the bank. The merchant does not need to know the customer's credit card number, and the bank does not need to know the details of the customer's order
* The customer is afforded extra protection in terms of privacy by keeping these two items separate.
* The two items must be linked and the link is needed so that the customer can prove that this payment is intended for this order and not for some other goods or service.



Purchase Request

1. Purchase-related information

2. Order-related information

3. Cardholder certificate.

Purchase Request Validation

1. verifies cardholder certificates using CA sigs

2. verifies dual signature using customer's public signature key

3. processes order and forwards the payment information to the payment gateway for authorization

4. sends a purchase response to cardholder