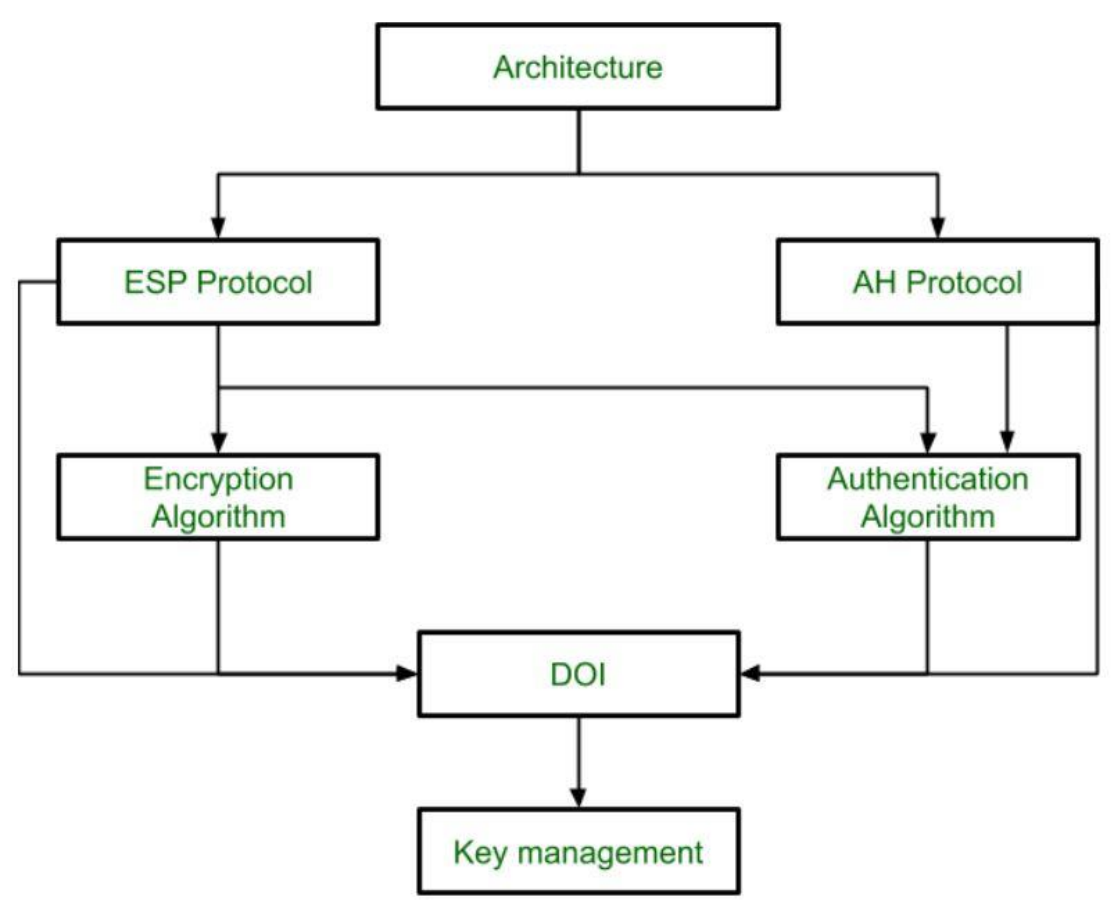
IP Security

IPsec

- **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 includes 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:

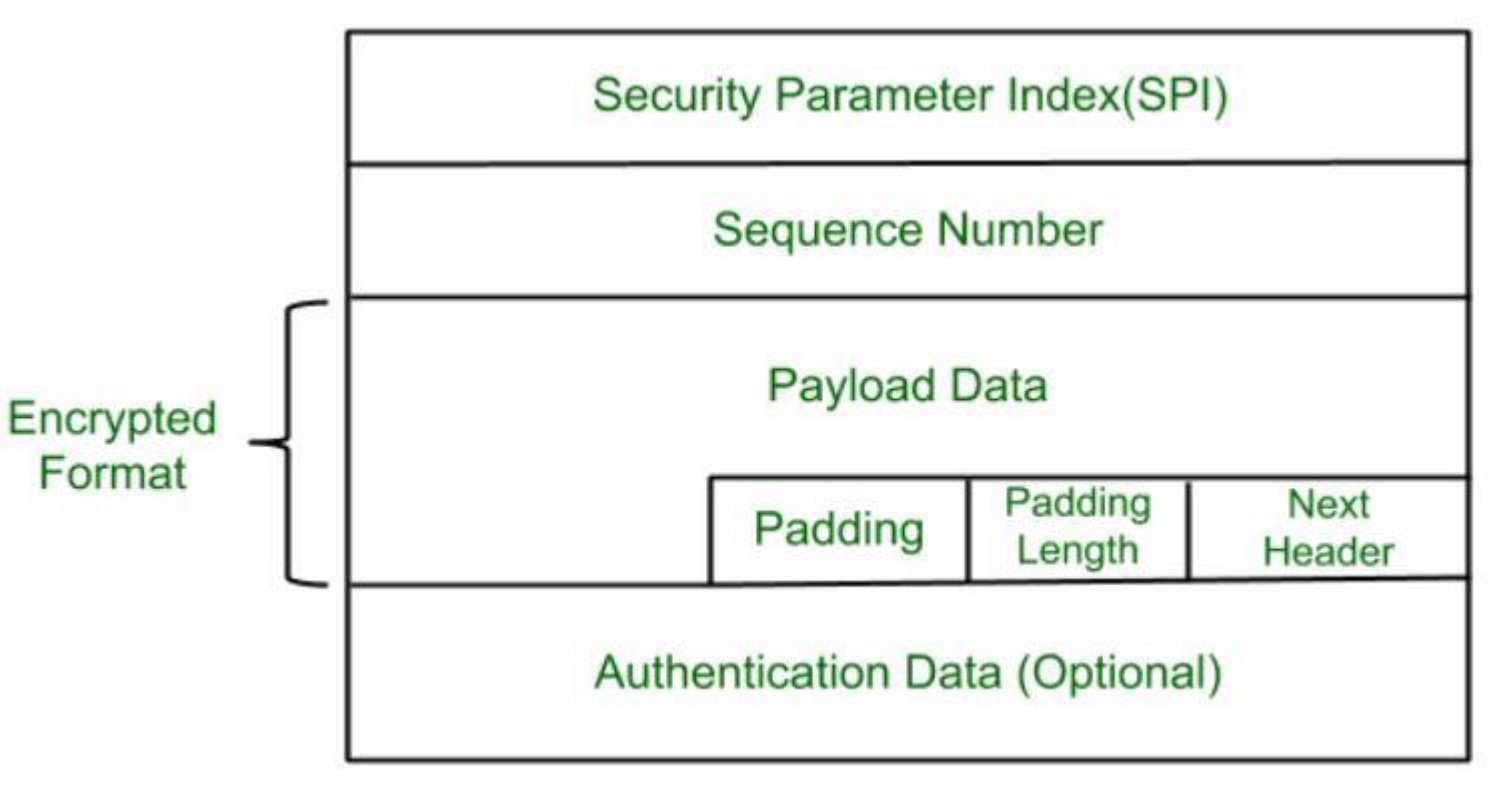


1. **Architecture:** Architecture or IP Security Architecture covers the general concepts, definitions, protocols, algorithms, and security requirements of IP Security technology.
2. **ESP Protocol:** ESP (Encapsulation Security Payload) provides a confidentiality service. Encapsulation Security Payload is implemented in either two ways:

   ESP with optional Authentication.

   ESP with Authentication.

Encapsulation Security Payload



Encapsulation Security Payload

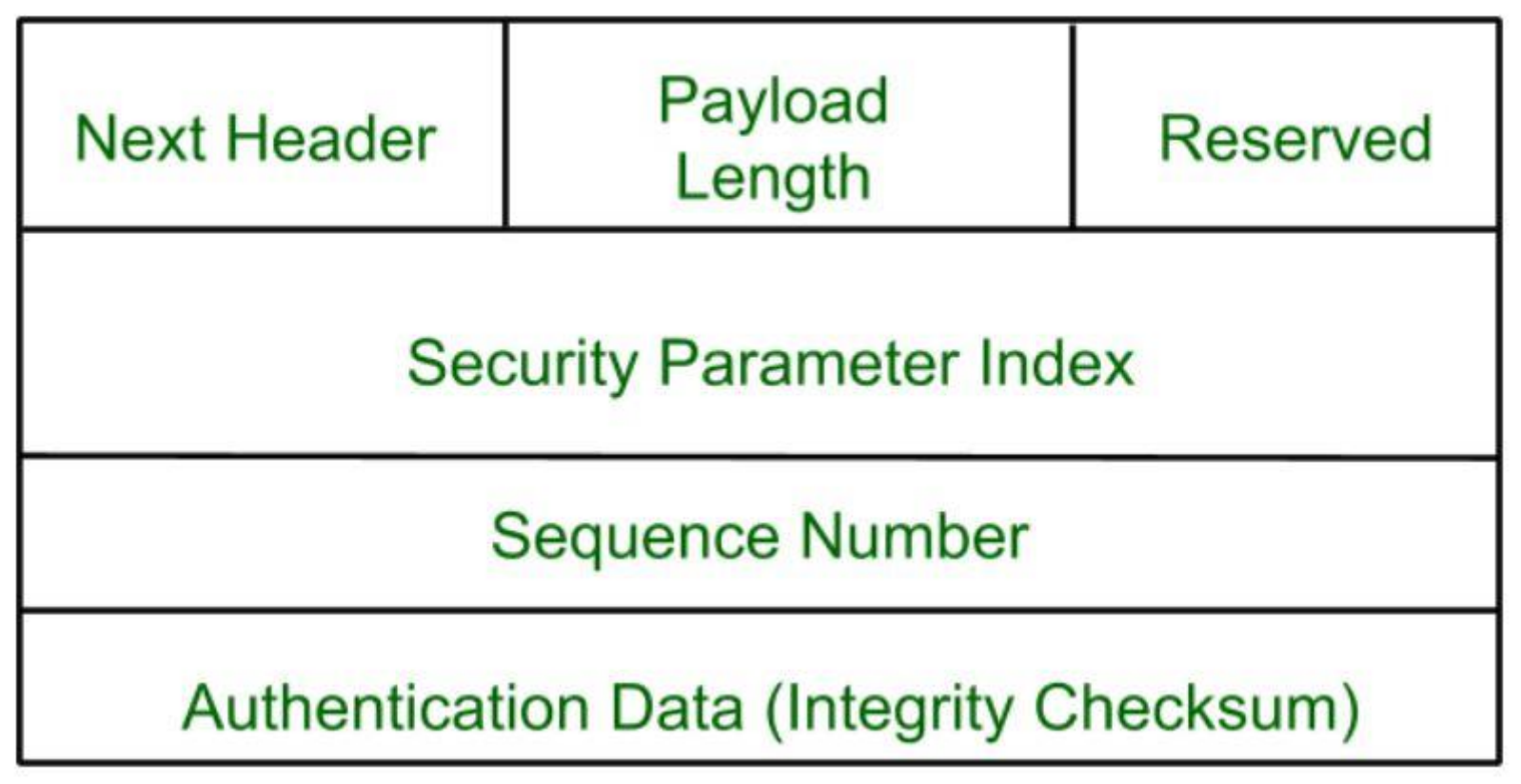
- **Security Parameter Index(SPI):** This parameter is used by Security Association. It is used to give a unique number to the connection built between the Client and Server.
- **Sequence Number:** Unique Sequence numbers are allotted to every packet so that on the receiver side packets can be arranged properly.
- **Payload Data:** Payload data means the actual data or the actual message. The Payload data is in an encrypted format to achieve confidentiality.
- **Padding:** Extra bits of space are added to the original message in order to ensure confidentiality. Padding length is the size of the added bits of space in the original message.
- **Pad Length (8 bits):** Indicates the number of pad bytes immediately preceding this field.
- **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: The encryption algorithm is the document that describes various encryption algorithms 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 issues related to the use of AH for packet authentication and integrity.

AH Format


Next Header
Payload Length
Reserved
Security Parameter Index
Sequence Number
Authentication Data (Integrity Checksum)

The fields are as follows –

- **Next header:** It is an 8-bit field which identifies the type of what follows. The value of this field is chosen from the set of IP header protocol fields, which is set to 51, and the value that would have gone in the protocol field goes in the AH next header field.
- **Payload length:** It is an 8 bits long field and contains the length of the AH header expressed in 32-bit words, minus 2. It does not relate to the actual payload length of the IP packet. Suppose if default options are used, the value is 4 (three 32-bit fixed words plus three 32-bit words of authentication data minus two).

- **Reserved (16 bits):** Reserved for future use (all zeroes until then).
- **Security Parameters Index (32 bits):** Arbitrary value which is used (together with the destination IP address) to identify the security association of the receiving party.
- **Sequence Number (32 bits):** A monotonic strictly increasing sequence number (incremented by 1 for every packet sent) to prevent replay attacks. When replay detection is enabled, sequence numbers are never reused, because a new security association must be renegotiated before an attempt to increament the sequence number beyond its maximum value.
- **Integrity Check Value (multiple of 32 bits):** Variable length check value. It may contain padding to align the field to an 8-octet boundary for IPv6, or a 4-octet boundary for IPv4.

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

6. DOI (Domain of Interpretation): DOI is the identifier that supports 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.

Thank You