

# Kryptolåda

## Inledning

Detta dokument beskriver en kryptolåda som kan sättas med utsida mot det publika Internet (enligt Internetspecifikationen) och på sin insida erbjuda paketförmedling enligt Internetspecifikationen med trafikskydd och textskydd.

En kryptolåda ska given en paketförmedlingstjänst enligt Internetspecifikationen kunna hitta andra kryptolådor för att upprätta relevanta koppel.

## Avhängighet

Detta dokument är beroende av Internetspecifikation.

## Begrepp

- **DoS-skydd:** Denial-of-service skydd från trafik som kommer från det publika Internet. En del av trafikskyddet.
- **Trafikskydd:** Ibland benämnt *signalskydd*, rör skydd av trafikflöden och behandlar bland annat störsändningar, falska meddelanden, och hoppande frekvenser / mottagaradresser.
- **Textskydd:** Ofta benämnt som kryptering, rör att skydda meddelandeinnehållet även om en antagonist kan läsa trafiken.

## Arkitektur

## Verifikation