0.1 Spezifikation des Schlüsselverteilungsprotokolls

Bei dem Schlüsselverteilungsprotokoll handelt es sich um ein einfaches Call-and-Response-Protokoll mit einem Roundtripp.

Verfahren

Nachrichtentyp „KDP-Request“

KDP-Request werden vom Client an den Server verschickt. Die Nachricht beinhaltet ein Typen-Feld, mit dem der Client die Art des Schlüsselmaterials bestimmt, und ein Feld mit der eigenen MAC-Adresse als Identifikator.

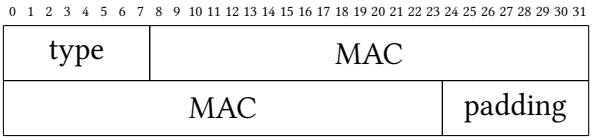

Abbildung 1: Aufbau einer KDP-Request-Nachricht

Nachrichtentyp „KDP-Response“

Das Typ-Feld aus dem KDP-Request bestimmt die Form des KDP-Response. In einer simplifizierten Form existieren KDP-Responses für die beiden Modi „client-driven“ und „server-driven“.

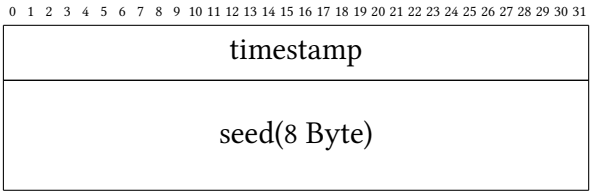

Abbildung 2: Aufbau einer KDP-Response-Nachrichten für die „client-driven“-Variante

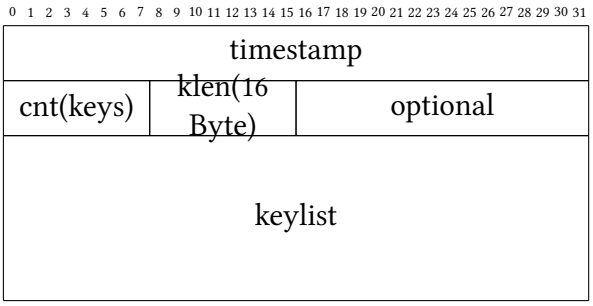

Abbildung 3: Aufbau einer KDP-Response-Nachrichten für die „client-driven“-Variante