Modul 7:
SCTP – Stream Control Transmission Protocol

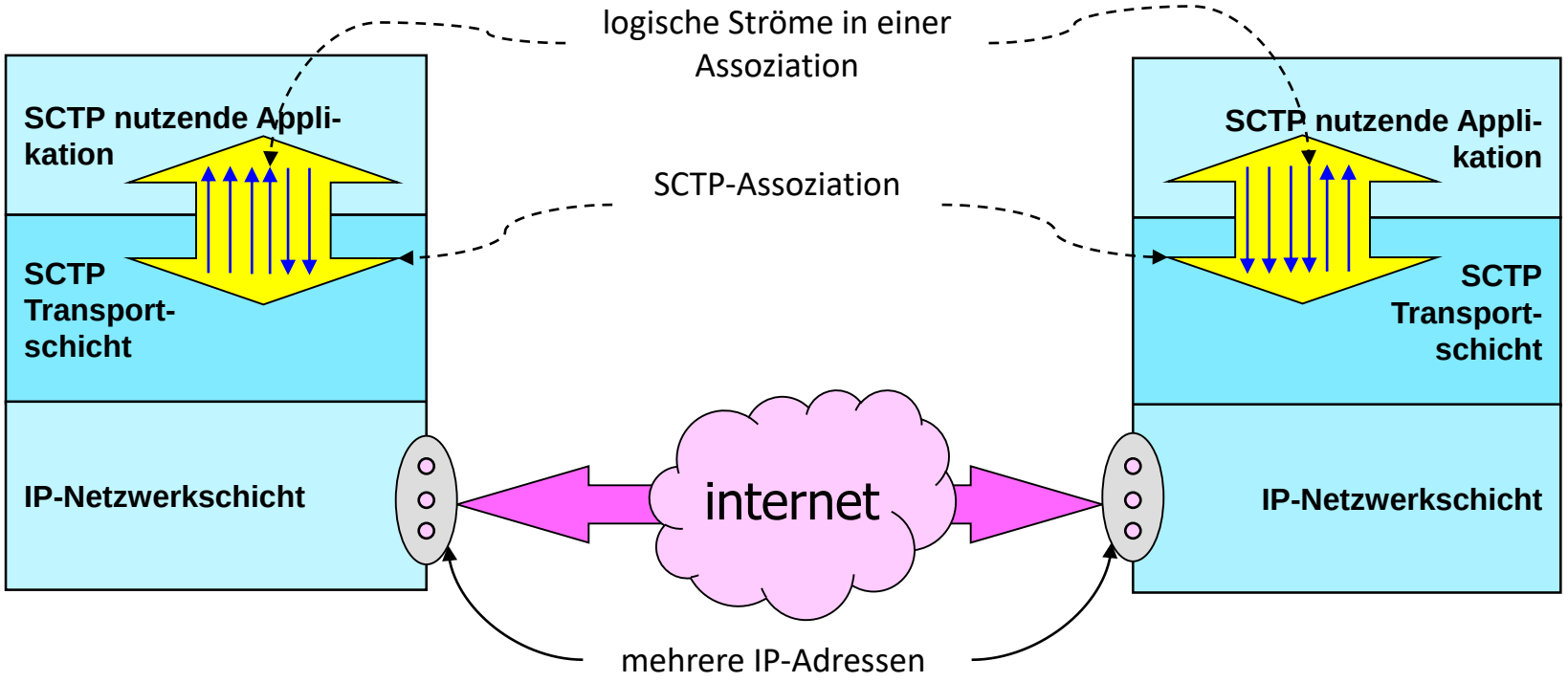
1. Geschichte, Motivation und Überblick
2. Hauptmerkmale
3. PDU-Format
4. Verbindungsmanagement
5. Erweiterungen
6. Vergleich TCP, UDP und SCTP

Geschichte, Motivation und Überblick

- TCP und UDP klassische Transportprotokolle (späte 60er Jahre)
  - UDP: unzuverlässiger Paketdienst; geeignet für Multicast und Broadcast
  - TCP: zuverlässiger, byteorientierter, unicast Streamingdienst
- Spezielle Anforderungen beim Transport von Signalisierungsdaten im Sprachverkehr führte zur Entwicklung des SCTP-Protokolls
  - Unterstützung eines Nachrichtenkonzepts
  - Konsequente Nutzung von SACK
  - Unterstützung von mehreren unabhängigen Nachrichtenströmen (Problem „Head of Line Blocking“ bei TCP)
  - Unterstützung alternativer Netzwerkpfade
  - Überwachung der Netzwerkpfade und Endpunkte
  - Optionale Reihenfolgesicherung
  - Sicherer Verbindungsaufbau (DoS-Angriffe)
- Oktober 2000: Die Signaling Transport (SIGTRAN) Gruppe der Internet Engineering Task Force (IETF) definiert im RFC 2960 das Stream Control Transmission Protocol
- Aktuelle Version: RFC4960 Stream Control Transmission Protocol, 09/2007

SCTP-Transportarchitektur

- **Konzept der Assoziation, die mehrere logische Ströme umfasst**
- **Unterstützung von Multihoming:**
  → für eine Zieladresse können mehrere IP-Adressen hinterlegt sein



SCTP-Überblick

SCTP ist ein Allzwecktransportprotokoll, das viele Vorteile und Eigenschaften von UDP und TCP enthält, kombiniert und erweitert:

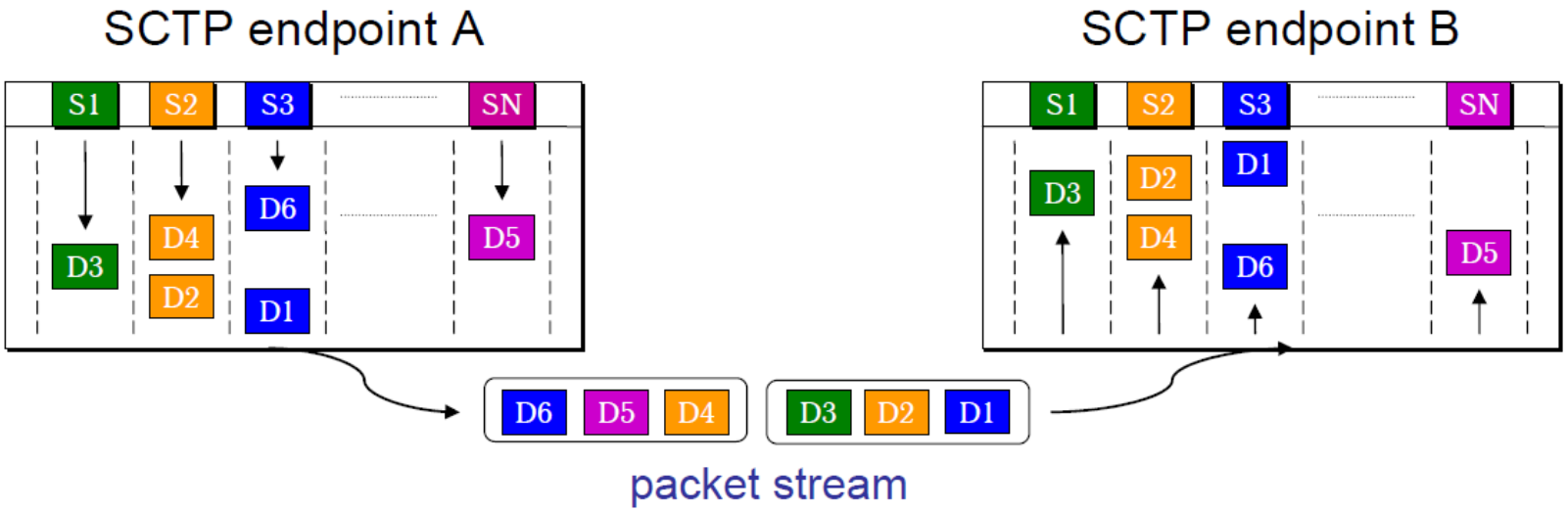
- **SCTP ist ein zuverlässiges, verbindungsorientiertes Transportprotokoll.**
- **SCTP kombiniert z.B. die paketorientierte Nachrichtenübermittlung von UDP mit Reihenfolgensicherung und Zuverlässigkeit.**
- **Reihenfolgensicherung kann bei Bedarf abgeschaltet werden → flexiblere Nachrichtenzustellung.**
- **Eine SCTP-Assoziation kann eine 1-zu-n Kommunikationsrelation zur Verfügung stellen („UDP style“).**
- **Eine Applikationen kann über eine SCTP-Transportassoziation mehrere unabhängige Datenströmen nutzen.**
- **Ein Datenstrom ist ein unidirektionaler logischer Kanal, der eine Folge von Nachrichten transportiert („Preservation of message boundaries“)**
- **Die Nachrichten (=SCTP-Informationseinheiten) werden in („getypten“) Chunks transportiert.**
  (Daten Chunk: Payload Data (DATA).
  Control Chunks: z.B. Initiation (INIT), Selective Acknowledgement (SACK))
- **Ein Chunk kann auf mehrere IP-Pakete verteilt werden und umgekehrt kann ein IP-Paket mehrere Chunks enthalten.**
- **Ein SCTP-Endpunkt kann mehrere IP-Adressen besitzen. Damit können zum Transport mehrere Pfade genutzt werden (Redundanz)**

Aufgaben der Control Chunks

Die Control Chunks werden genutzt zur

- **zur Steuerung des Verbindungsaufbaus,**
- **zur Steuerung des Verbindungsabbaus,**
- **zur Bestätigung von empfangenen Nutzdaten,**
- **für die Überwachung der Erreichbarkeit des assoziierten Endpunkts,**
- **für die Überwachung des Status von Netzwerkpfaden zum assoziierten Endpunkt,**
- **zur Übertragung von Fehlermeldungen,**
- **zur Konfiguration der Multihoming-Adressen,**
- **für weiteren optionalen Protokollerweiterungen.**

Multi-Streaming

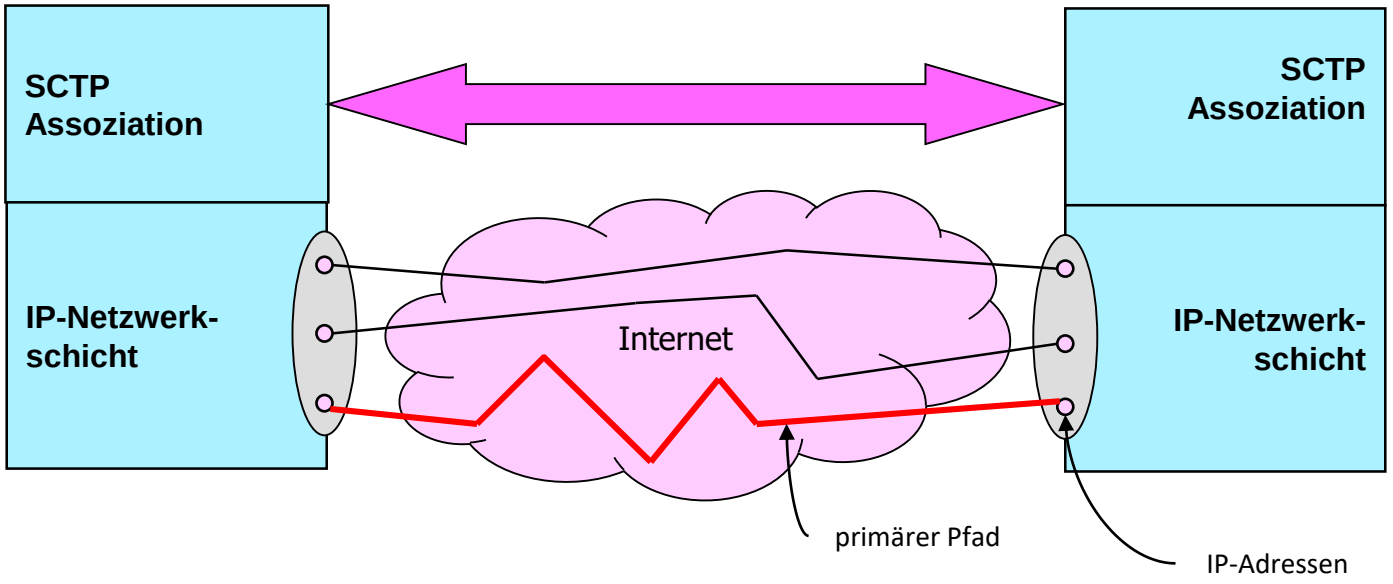


aus: Unurkhaan, Esbold: Secure End-to-End Transport over SCTP - A new security extension for SCTP, Dissertation; 2005

- **Kein Head of Line Blocking:**
  Übertragung der Nutzdaten erfolgt über unabhängige Kanäle bzw. Streams.
  Der Verlust eines Chunks beeinflusst nur einen Stream und nicht die anderen Streams.

Multi-Homing

- Zuordnung von mehrere IP-Adressen zum Endpunkt einer Assoziation (Port bleibt gleich).
- Dadurch sind mehrere Pfade möglich; für jeden Pfad wird ein kompletter Parametersatz für Fluss- und Überlastkontrolle gehalten.
- Ein ausgesuchter Pfad (primärer Pfad) überträgt Daten, die restlichen Pfade sind redundant und werden bei Bedarf aktiviert (Failover).



Bundling + User Data Fragmentation

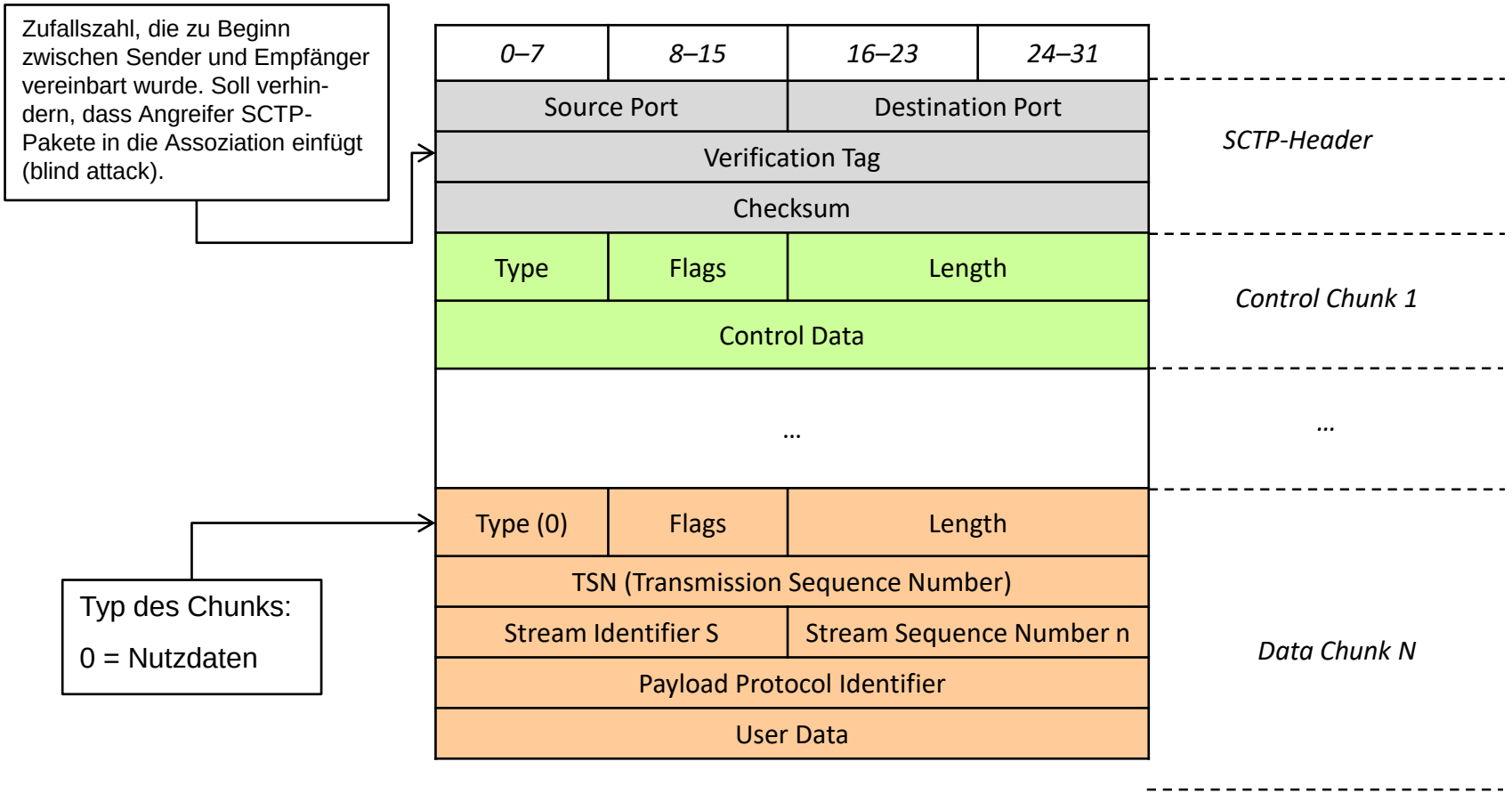
Bundling bedeutet: mehrere Chunks können in einem SCTP-Paket transportiert werden.

- **Jedes SCTP-Paket beginnt mit einem „Common Header“.**
- **Bundling ist ein optionales Merkmal**
- **Die Control Chunks kommen in einem SCTP-Paket vor den Data Chunks**
- **Einige Control Chunks, wie z.B. INIT, INIT-ACK dürfen nicht „gebundelt“ werden.**

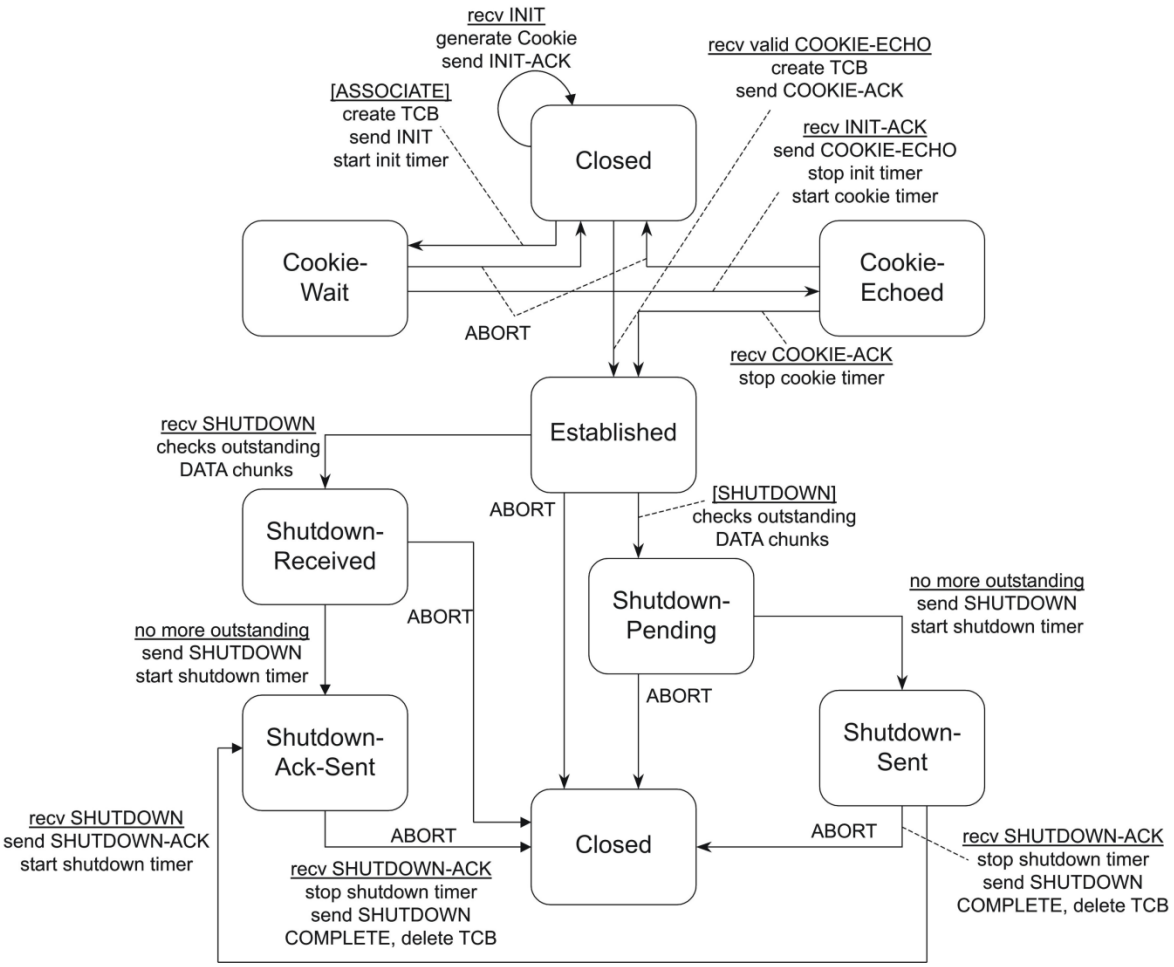
Wenn ein Data Chunk größer als die verwendete MTU ist, können die Benutzerdaten fragmentiert werden.

TSN (Transmission Sequence Number) nummeriert fortlaufend (stream-unabhängig) Data Chunks (→ Acknowledgement, → Duplikat-Erkennung). Stream Sequence Number nummeriert fortlaufend die Chunks in einem Stream.

SCTP - PDU-Format

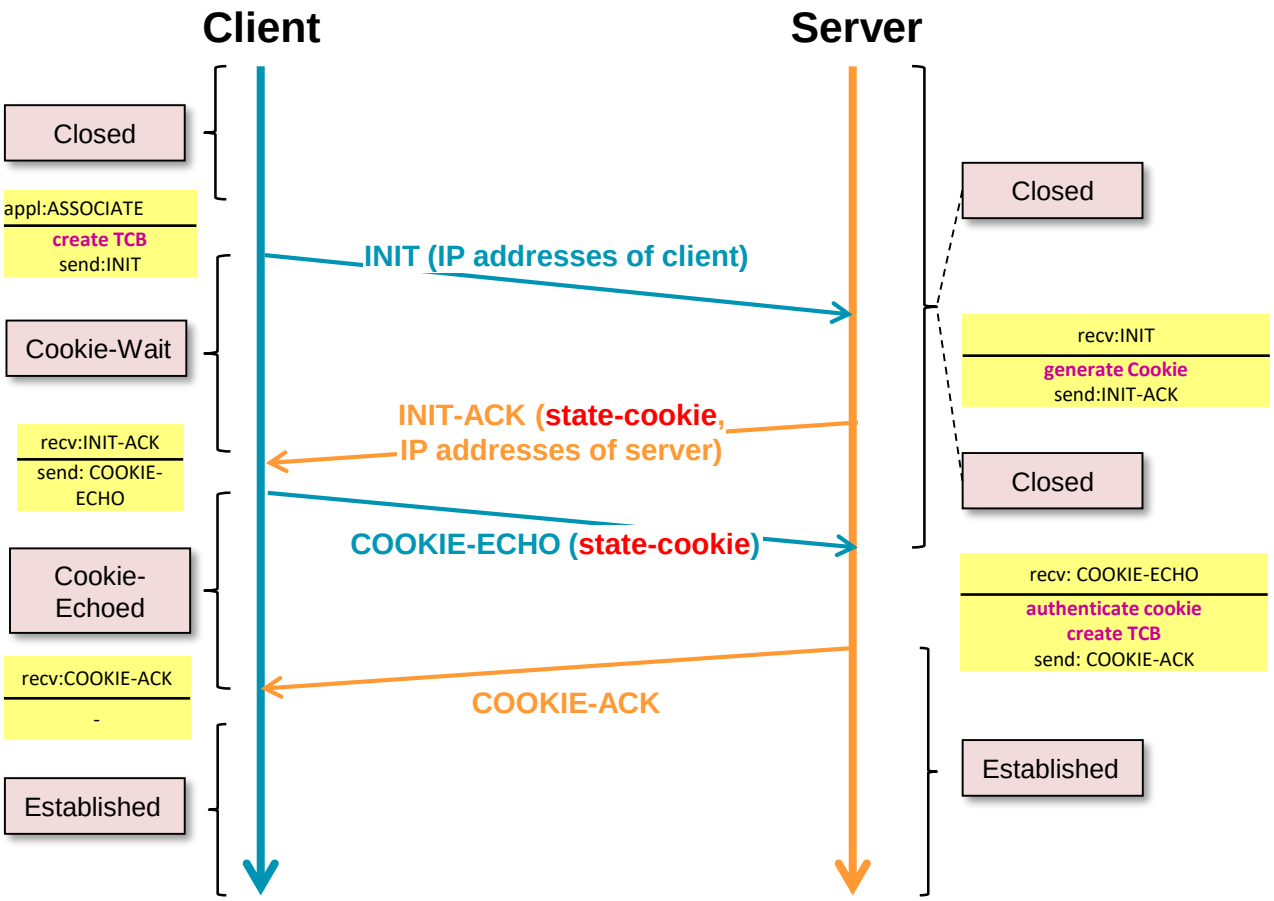


SCTP-Verbindungsmanagement



aus: Unurkhaan, Esbold: Secure End-to-End Transport over SCTP - A new security extension for SCTP, Dissertation; 2005

Normalfall SCTP-Verbindungsaufbau (4-way handshake)



state-cookie enthält alle Informationen, die sich auf die Assoziation beziehen, so dass keine Ressourcen allokiert werden müssen. (→ DoS-Attacke)

Nach Senden des INIT-ACK bleibt Server unverändert in Zustand Closed.

Gesichert wird das Cookie durch folgende „keyed-hashed“ Werte:

- **timestamp**
- **INIT PDU**
- **INIT-ACK PDU**

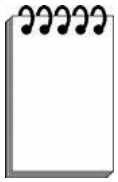
TCB = Transmission Control Block (Kontext der Assoziation)

SCTP Erweiterungen

- **ADD-IP: dynamische Rekonfiguration einer existierenden Assoziation:**
  Erlaubt im Wesentlichen folgende Konfigurationsänderungen:
  - Hinzufügen einer neuen IP-Adresse,
  - Löschen einer alten IP-Adresse und
  - Setzen eines neuen Primärpfads zum assoziierten Endpunkt.
- **Concurrent Multipath Transfer for SCTP (CMT-SCTP)**
- **Teilgesicherte Transportmodus (PR-SCTP):**
  statt einer Neuübertragung eines oder mehrerer verloren gegangener Daten-Chunks wird einen neuer Chunk-Typen gesendet, der der Gegenseite anzeigt, dass sie „weitermachen“ soll.
- **Nachrichten mit variabler Lebenszeit:**
  Feingranulare Steuerung der Zuverlässigkeit, bei Multimediakommunikation.
- **Mobilitätsunterstützung:**
  Kombination von Mobile-IP und Mobile-SCTP (ADD-IP), um durch simultanen Handoff eine bestehende Assoziation bei Ortwechsel aufrecht zu erhalten.

UDP vs. TCP vs. SCTP

Services/Features	UDP	TCP	SCTP
Connection-oriented	no	yes	yes
Full duplex	yes	yes	yes
Reliable data transfer	no	yes	yes
Partial-reliable data transfer	no	no	optional
Ordered data delivery	no	yes	yes
Unordered data delivery	yes	no	yes
Flow control	no	yes	yes
Congestion control	no	yes	yes
ECN capable	no	yes	yes
Selective ACKs	no	optional	yes
Preservation of message boundaries	yes	no	yes
Path MTU discovery	no	yes	yes
Application PDU fragmentation	no	yes	yes
Application PDU bundling	no	yes	yes
Multistreaming	no	no	yes
Multihoming	no	no	yes
Protection against SYN flooding attacks	n/a	no	yes
Allows half-closed connections	n/a	yes	no
Reachability check	no	yes	yes
Psuedo-header for checksum	yes	yes	no (uses vtags)
Time wait state	n/a	yes (conn. shutdown)	no (uses vtags)



aus: http://www.isoc.org/briefings/017/