Vorlesung

Methodische Grundlagen des Software-Engineering

im Sommersemester 2014

Prof. Dr. Jan Jürjens

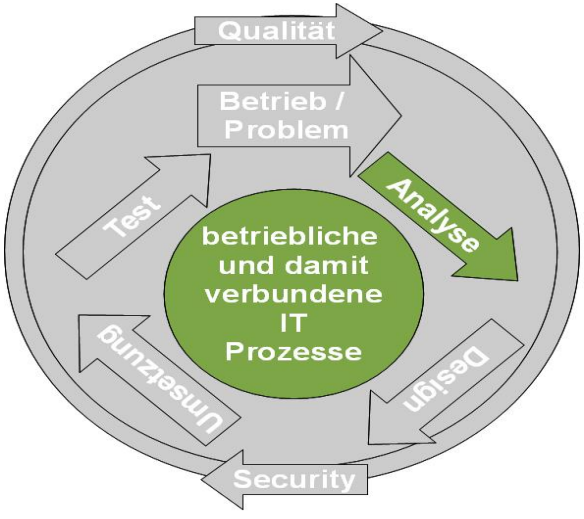
TU Dortmund, Fakultät Informatik, Lehrstuhl XIV

Teil 3.5: Kryptographische Protokolle

v. 08.07.2014

Einordnung
3.5 Kryptographische Protokolle

- Geschäftsprozessmodellierung
- Process-Mining
- Modellbasierte Entwicklung sicherer Software
  - Einführung: Software Security
  - Hintegrund IT-Sicherheit
  - Wiederholung: Modellbasierte Software Entwicklung
  - Modellbasierte Sicherheit mit UML
  - Sichere Architekturen
  - Kryptographische Protokolle
  - Protokollanalyse
  - Biometrische Authentisierung
  - Biometrische Authentisierung: Analyse
  - Elektronische Geldbörsen
  - Clouds
  - Elektronische Signatur
  - Bankarchitektur



Literatur:
[Jür05] Jan Jürjens: **Secure systems development with UML**, Springer-Verlag 2005.
Unibibliothek (e-Book):
http://www.ub.tu-dortmund.de/katalog/titel/1361890
Papier-Version:
http://www.ub.tu-dortmund.de/katalog/titel/1091324
Kap. 5

- **Letzter Abschnitt:** sichere Architekturen
  - Guarded Objects
  - no down-flow, data security
- **Dieser Abschnitt:** Kryptographische Protokolle
  - Probleme von Sicherheitsprotokollen
  - ISO OSI Schichten-Modell
  - Sicherheitsanalyse
  - Kryptographische Ausdrücke

Sicherheitsprotokolle

- System über **nicht vertrauenswürdiges** Netzwerk verteilt.
- Angreifer kann Nachrichten abfangen, modifizieren, löschen und einfügen.
- **Kryptographie** ermöglicht Sicherheit.
- **Kryptographisches Protokoll:**
  - Austausch von **Nachrichten**
  - für verteilte Sitzungsschlüssel, authentisierenden Auftragsgebern...
  - durch Benutzung von **kryptographischen** Algorithmen.
- Korrekter Entwurf sehr schwierig.

Beispiel: Authentisierungs-Protokolle

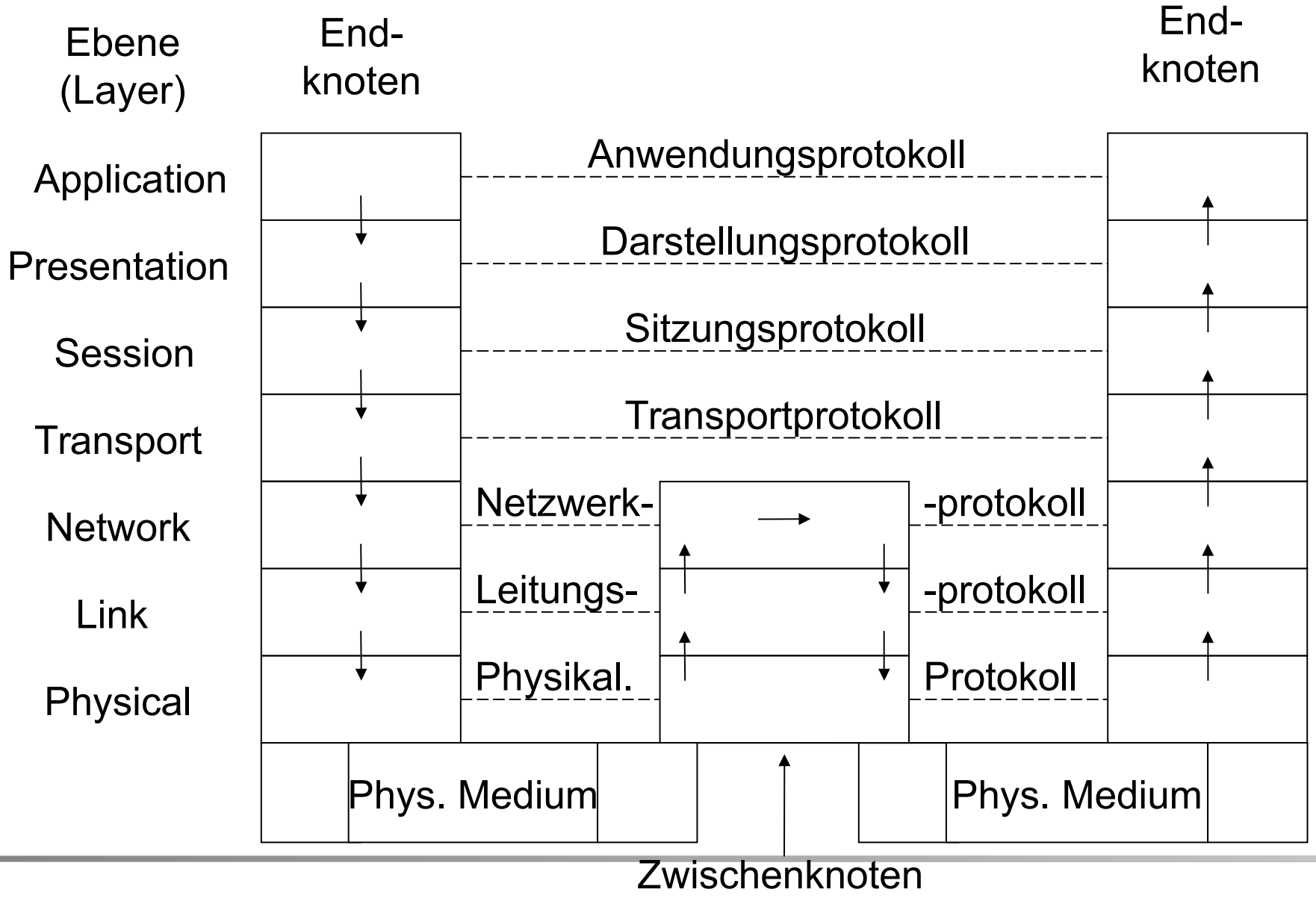
- Ziel: Sichere **Authentisierung** von Kommunikationspartnern.
- Bedrohungen:
  - **Fälschung** von Identitäten.
  - **Unautorisierte Verwendung** von Identitäten.
- Weitere Ziele von Sicherheitsprotokollen:
  - **Schlüsselmanagement,**
  - Elektronische **Transaktionen,** ...

Sicherheitsprotokolle: Probleme

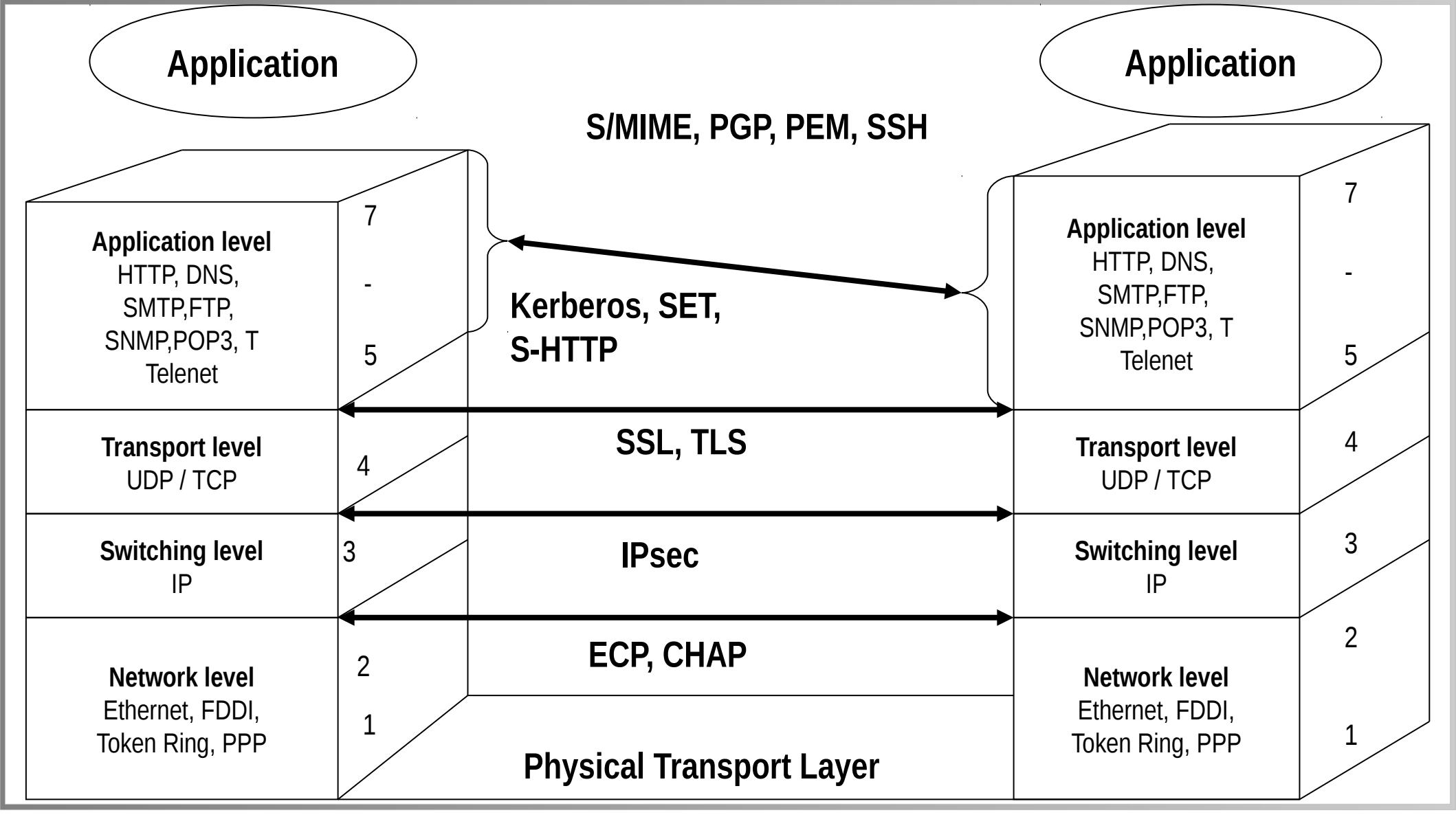
Schwachstellen vieler Protokolle aus verschiedenen Gründen:

- Schwache Kryptographie.
- **Zentraler Nachrichten-Austausch.**
- **Schnittstellen, Prologe, Epiloge.**
- Verwendung.
- Implementierungsfehler.

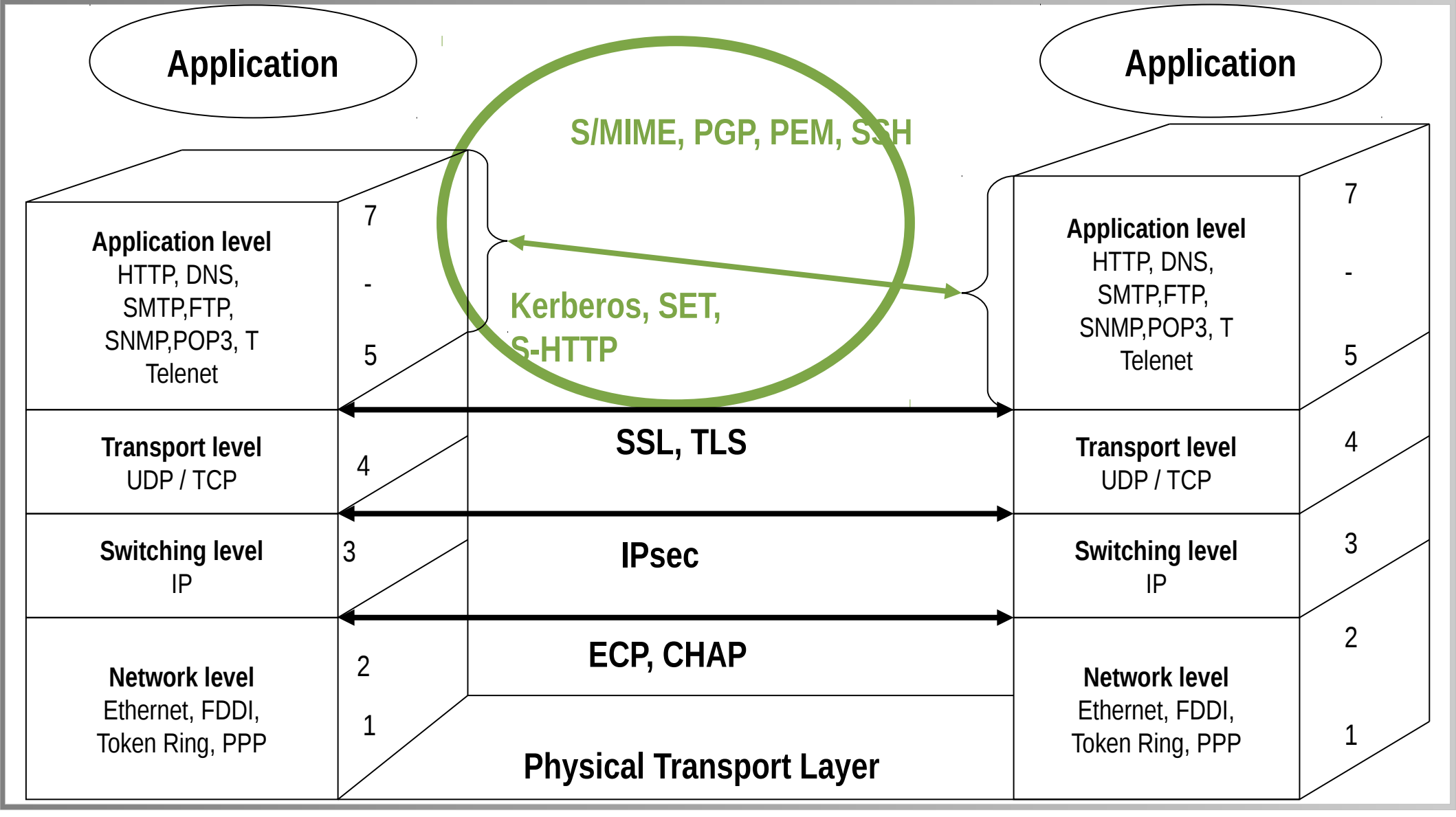
ISO OSI 7-Schichten-Modell



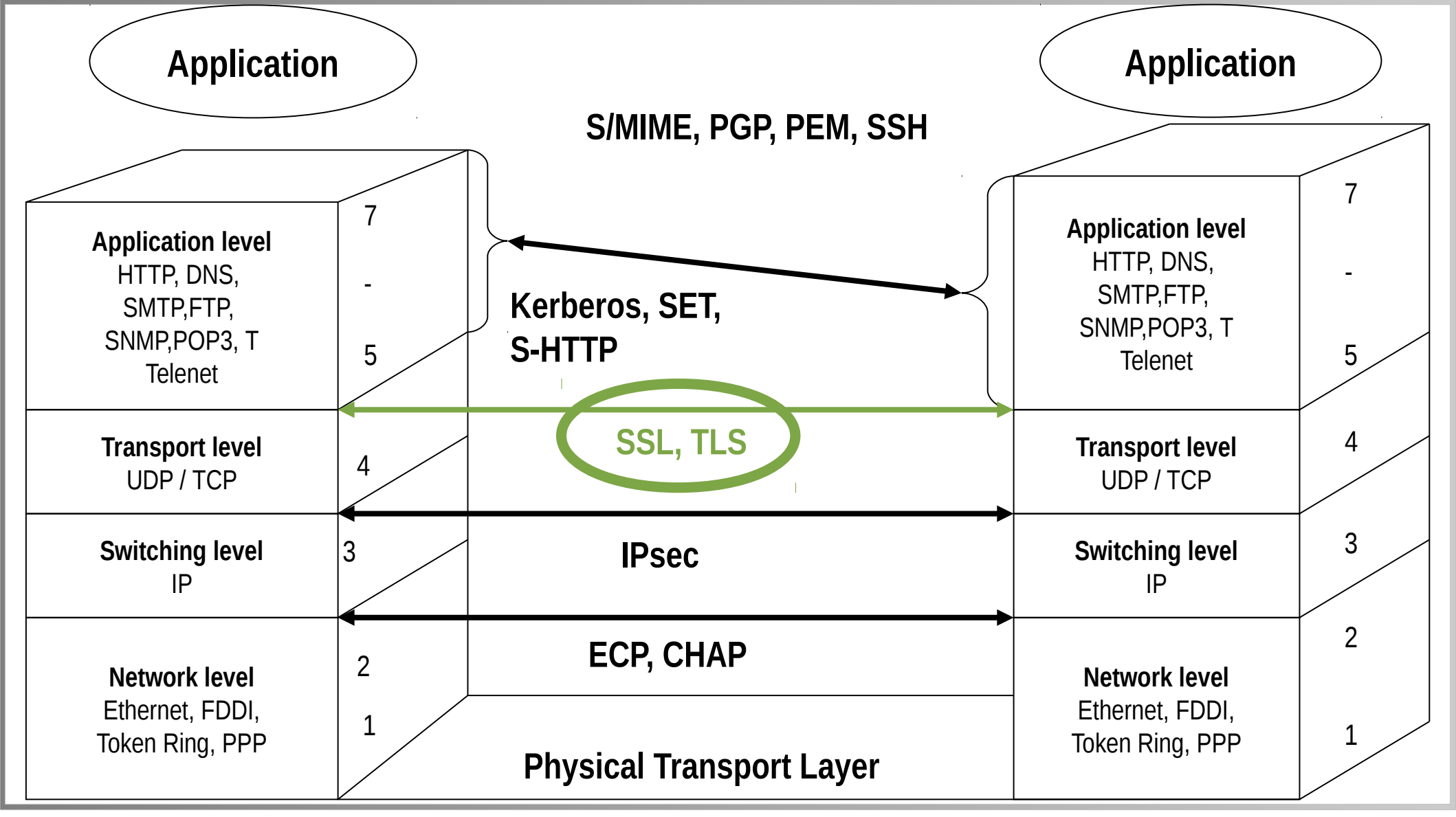
Verschlüsselung und Protokollebenen



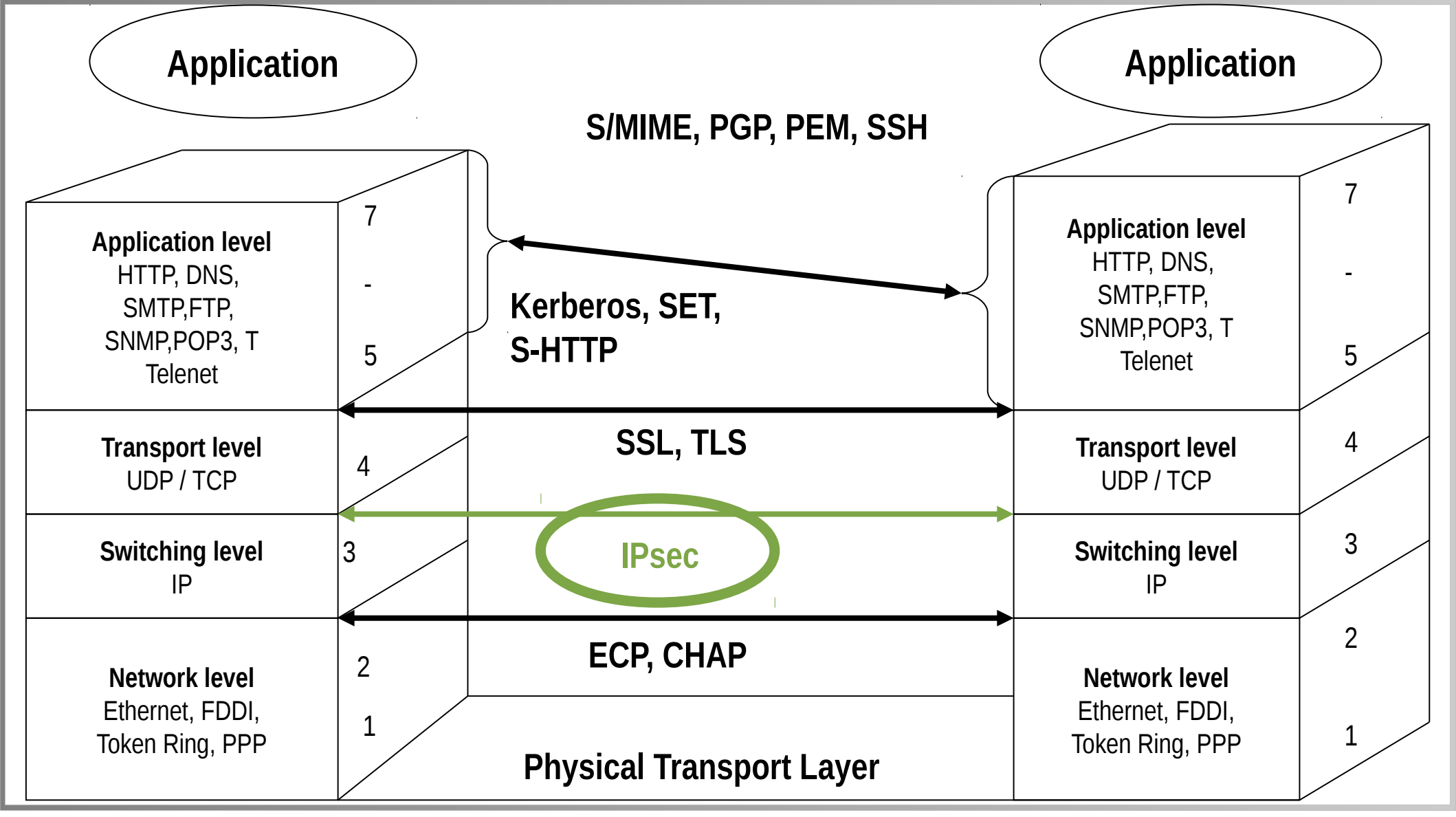
Verschlüsselung und Protokollebenen



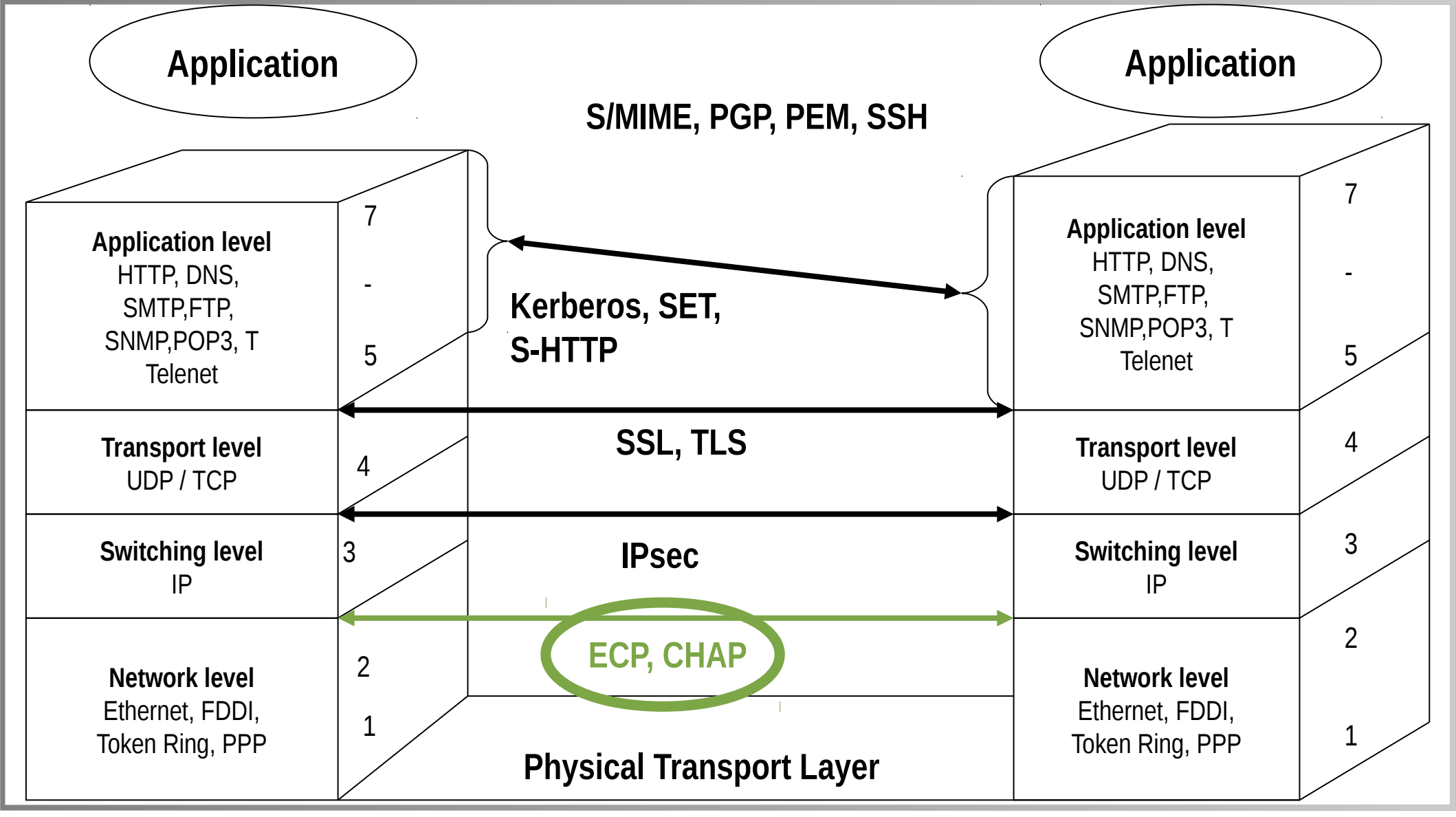
Verschlüsselung und Protokollebenen



Verschlüsselung und Protokollebenen



Verschlüsselung und Protokollebenen

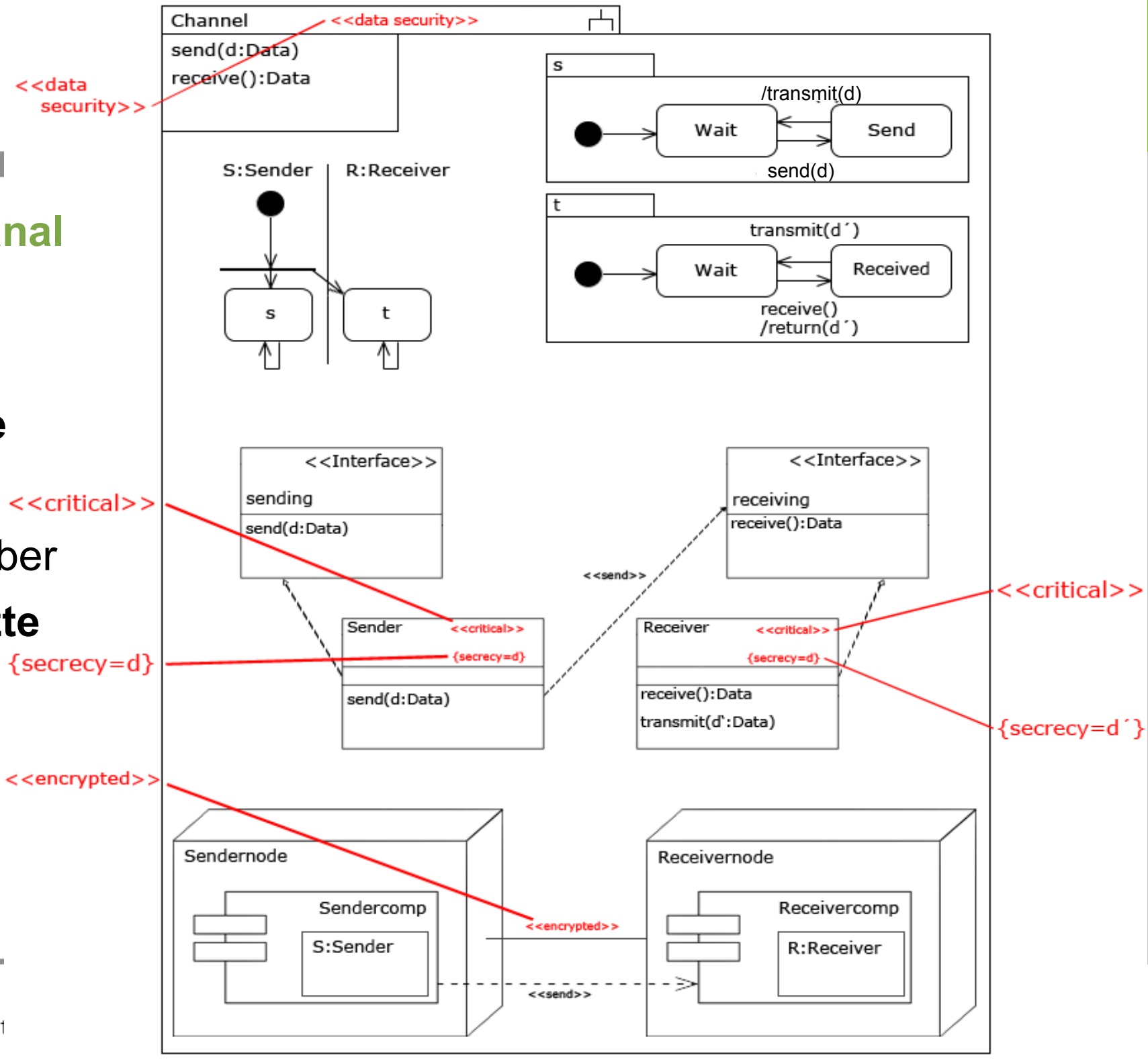


Beispiel:

Sicherer Kanal

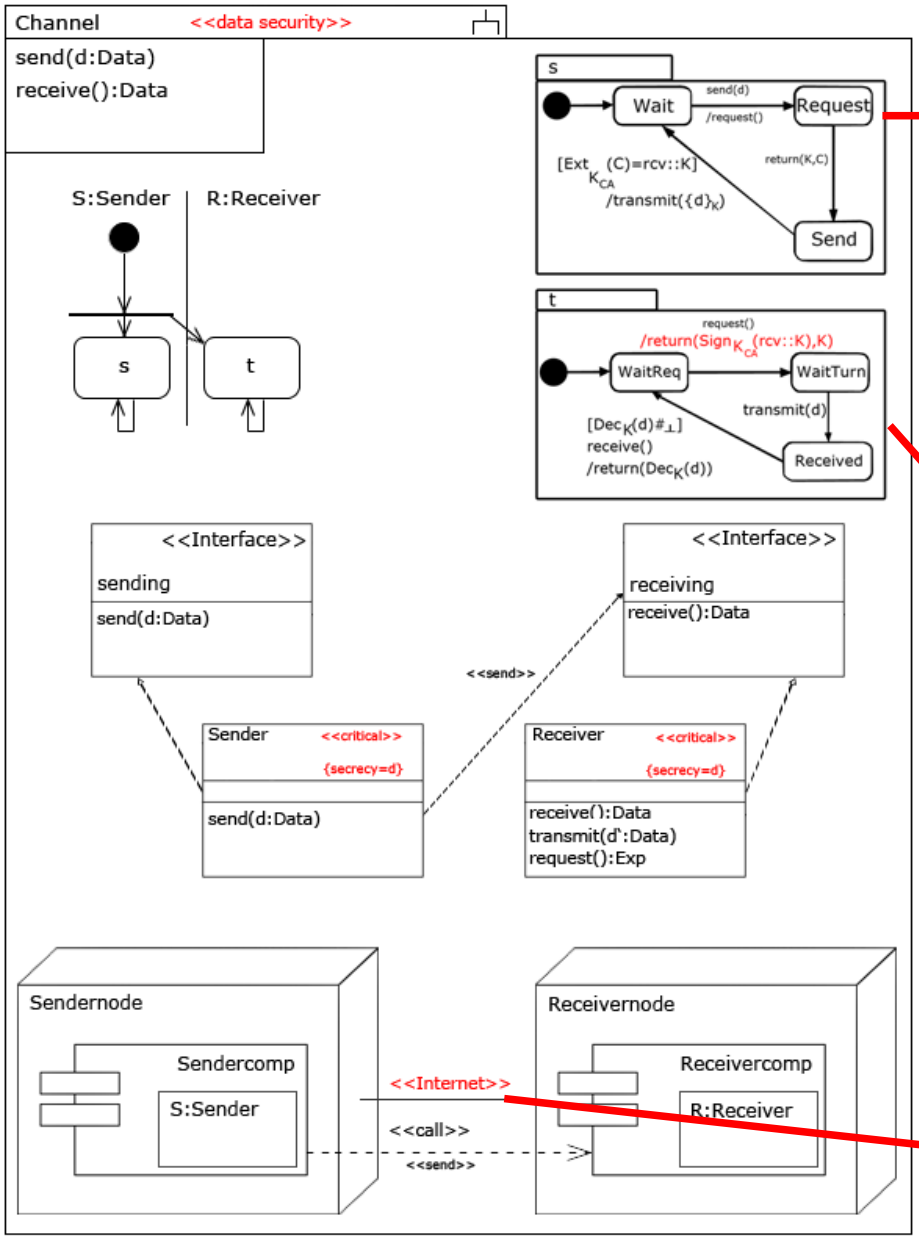
Ziel:

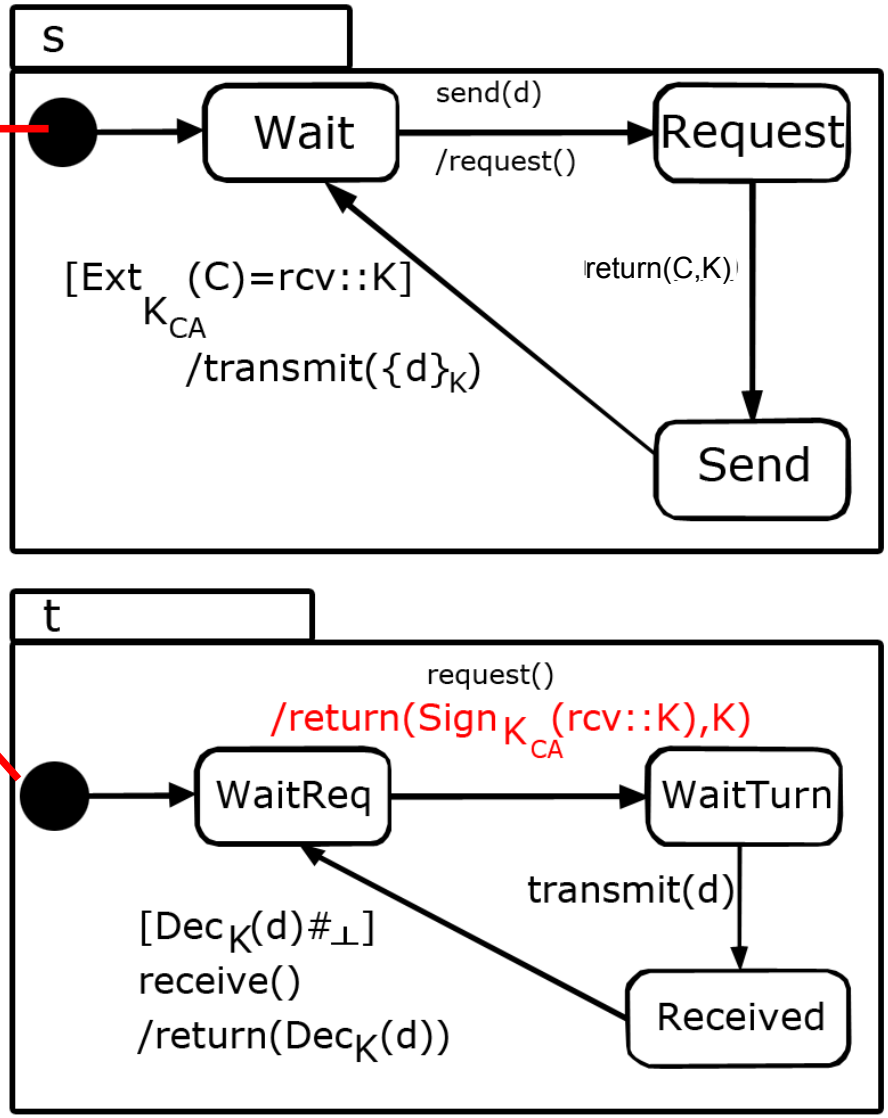
vertrauliche Übertragung von Daten über **ungeschützte** Kommuni-kations-verbindung



Sicherer Kanal: Protokoll

Verschlüsseln unter **Sitzungsschlüssel** nach Austausch eines **Zertifikates**.





<<Internet>>

ographische Pr

Sicherheitsanalyse

Nach Dolev, Yao (1982):

- Sicherheitsanalyse: **Verifiziere Systemmodell** gegen Angreifermodel.
- Auf Basis Bedrohungsszenarien in Verteilungsdiagrammen.
- Eigenschaften von Systemmodell:
  - Teilnahme an Protokollläufen.
  - Daten im Voraus **kennen.**
  - Nachrichten von Kommunikationsverbindungen **abfangen.**
  - Nachrichten in Kommunikationsverbindungen einfügen.
  - Zugriff auf System-Knoten.

Angreifer

- Verschiedene **Angreifer-Klassen greifen** unterschiedliche Stellen des Systems **an**.

  → Entsprechend der Gefährdungsszenarien.

- Beispiel: **Insider**-Angreifer kontrolliert Kommunikationsverbindungen im LAN.

- Für Sicherheitsanalyse der Spezifikation: Simulation zusammen mit gegebenem Angreifermodell.

Kryptographie

Im Kontext der Sicherheitsanalyse:

- Schlüssel = **Symbole.**
- Kryptoalgorithmen = **abstrakte** Operationen:
  - Nur mit **richtigen** Schlüsseln entschlüsselbar.
  - Keine **statistischen** Angriffe ausführbar.

Kryptographie: Schlüssel

- *Keys:* Folge mit partieller injektiver Abbildung:

  $( )^{-1} : Keys \rightarrow Keys$

- Schlüssel: unabhängig (Keine Gleichungen wie $K = K' + 1$ für zwei verschiedene Schlüssel $K, K' \in Keys$).
- Öffentlicher Schlüssel für Verschlüsselung und Überprüfung der Signatur benutzbar.
- Schlüssel, die für sicher gehalten werden, für Entschlüsselung und Unterzeichnung benutzbar.
- Schlüssel: entweder Verschlüsselungs- oder Entschlüsselungs-schlüssel (asymmetric), oder beides falls $k \quad k^{-1} = k0$ zufriedenstellt (symmetric).
- Zahlen von symmetrischen & asymmetrischen Schlüssel: unendlich.

Kryptographie: Keys, Var, Data

- *Var:* eine unendliche Folge von Variablen.
- *Data:* eine unendliche Folge von Datenwert.
- *Keys*, *Var* und *Data:* wechselseitig disjunkt.
- *Data* beinhaltet die Namen $UMNames \cup MsgNm$.
- *Data* kann auch nonces und andere secrets beinhalten.

Kryptographie: Quotient einer Termalgebra

Wdh.: Termalgebra durch Folge von Elementen & Operationen erzeugt.

→ Folge von Termen, gebildet durch Anwendung der Operationen auf Elementen.

Quotient der Termalgebra unter gegebenem Satz von Gleichungen abgeleitet durch:

- Einführung dieser Gleichungen und
- den von ihnen unter den Bedingungen abgeleiteten.

Algebra kryptographischer Ausdrücke *Exp*: Quotient der Termalgebra erzeugt durch die Folge:

$$Var \cup Keys \cup Data$$

Kryptographische Ausdrücke (1/3)

Exp: Menge der ***Krypto-Terme***

- Bildung aus Symbolen in Mengen *Data*, *Keys*, *Var*
- Unter Verwendung der Operationen:
  - *_::_* (Konkatenation), *head(_)*, *tail(_)*,
  - *(_)$^{-1}$* (K^{-1}: zum Verschlüsselungsschlüssel K gehöriger Entschlüsselungsschlüssel).
  - *{ _ }_* ($\{M\}_K$: Verschlüsselung der Nachricht M mit Schlüssel *K*) .
  - *Dec_( )* ($Dec_K(C)$: Entschlüsselung der Daten C mit Schlüssel *K*).
  - *Sign_( )* ($Sign_K(M)$: Signatur der Nachricht M mit Schlüssel *K*).
  - *Ext_( )* ($Ext_K(S)$: Extrahieren der Signatur S mit Schlüssel *K*).

Kryptographische Ausdrücke (2/3)

- Unter Berücksichtigung folgender Gleichungen:
  - $\forall E,K.\ Dec_K^{-1}(\{E\}_K)=E$
  - $\forall E,K.\ Ext_K(Sign_K^{-1}(E))=E$
  - $\forall E_1,E_2.\ head(E_1::E_2)=E_1$
  - $\forall E_1,E_2.\ tail(E_1::E_2)=E_2$
- Assoziativität für $::$.
- Bessere Lesbarkeit: schreibe $E_1::E_2::E_3$ für $E_1::(E_2::E_3)$ und $fst(E_1::E_2)$ für $head(E_1::E_2)$ etc.

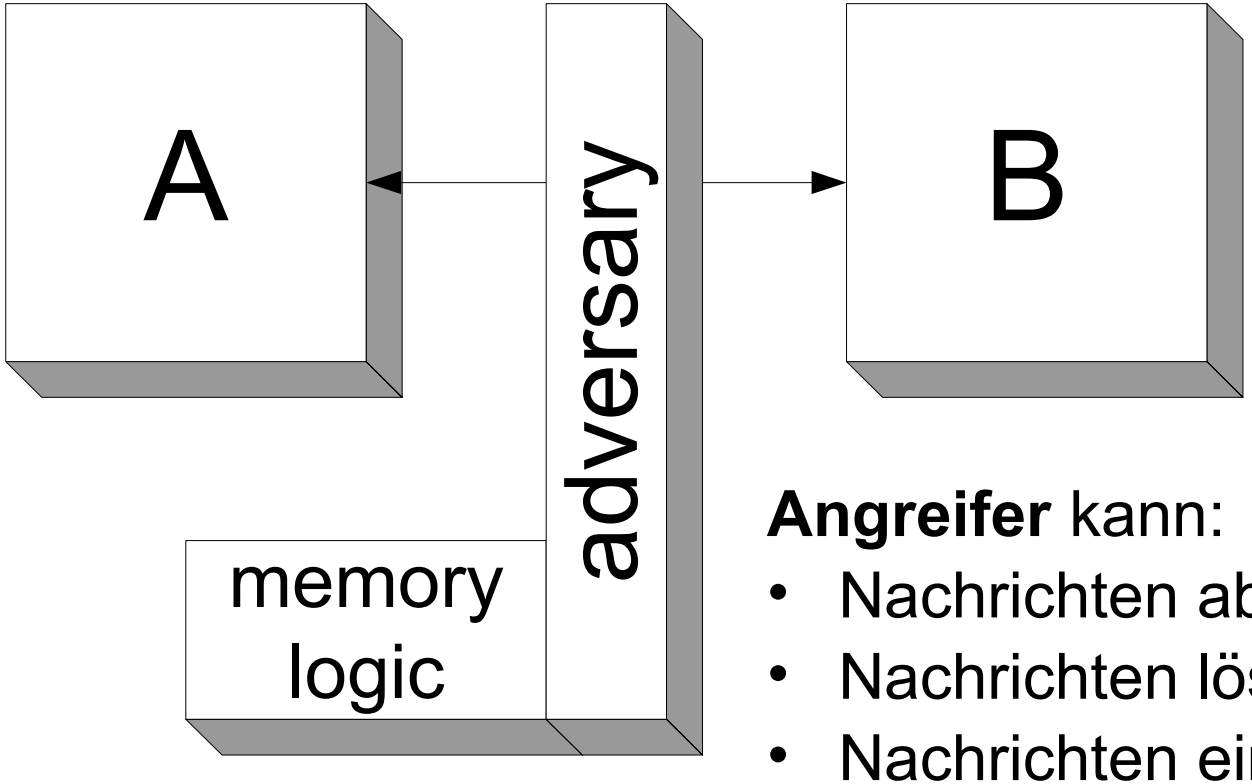
[NB: Bei Bedarf o.g. Gleichungen um weitere krypto-spezifische Eigenschaften erweiterbar (z.B. bei XOR).]

Kryptographische Ausdrücke (3/3)

- Für jede $E \in Exp$, folgende Abkürzungen benutzen:
  - $fst(E) =^{def} head(E)$
  - $snd(E) =^{def} head(tail(E))$
  - $thd(E) =^{def} head(tail(tail(E)))$
- Weitere kryptospezifische Grundelemente und Gesetze (XOR, …) einbeziehen.
- Abstraktes Model von kryptographischen Algorithmen: abstrahiert Details auf Ebene der Bitfolge weg. → Mechanische Analyse möglich.
- Anhand Formalisierung kryptographischer Operationen (freshness, secrecy, integrity, authenticity)
  - wichtige Voraussetzungen für sicherheitskritische Daten

  auf Ebene der UML Diagrammen in mathematischer präziser Art formulierbar.

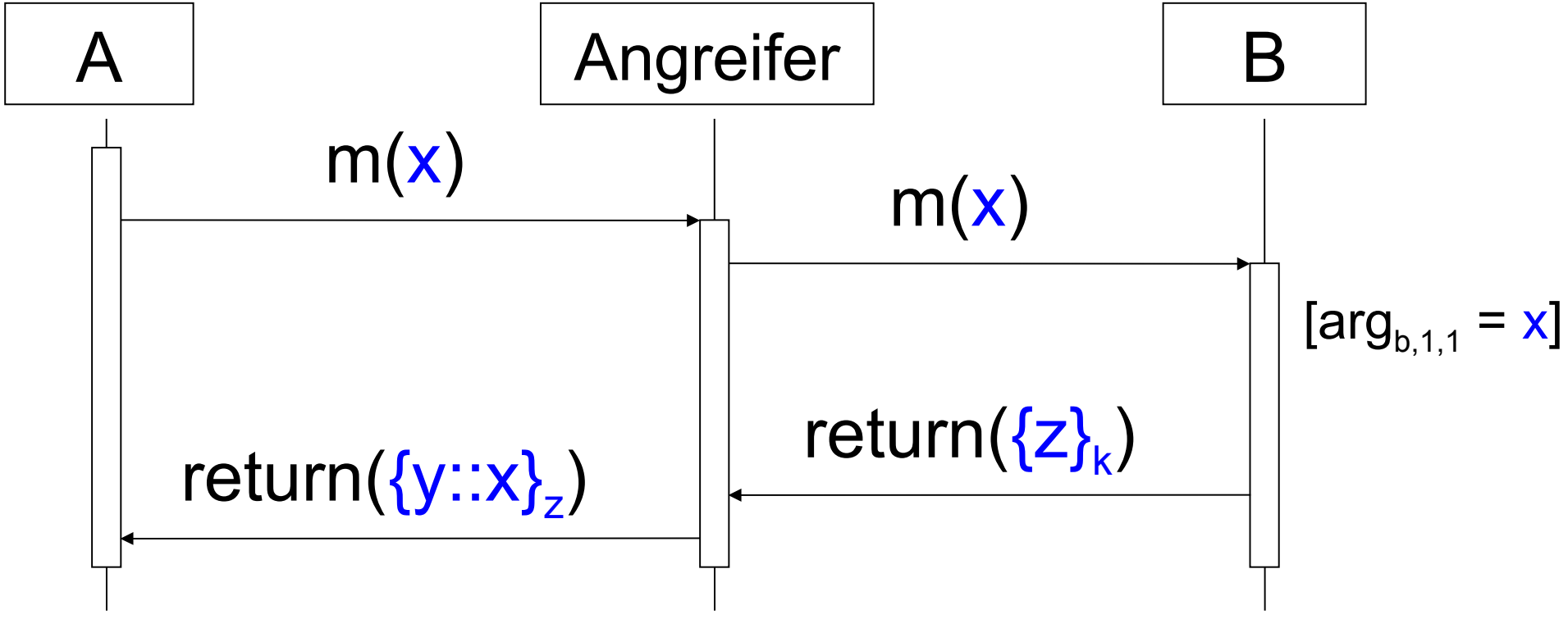
Angreifer-Modell



Angreifer kann:

- Nachrichten abspeichern.
- Nachrichten löschen.
- Nachrichten einfügen.
- Nachrichten erstellen.
- **Kryptographische Funktionen** benutzen.
- Bestimmte Systemknoten kontrollieren.
- Bestimmte Daten vorab kennen.

Kryptobasierte Software (z.B Protokolle)



Angreifer-Wissen:

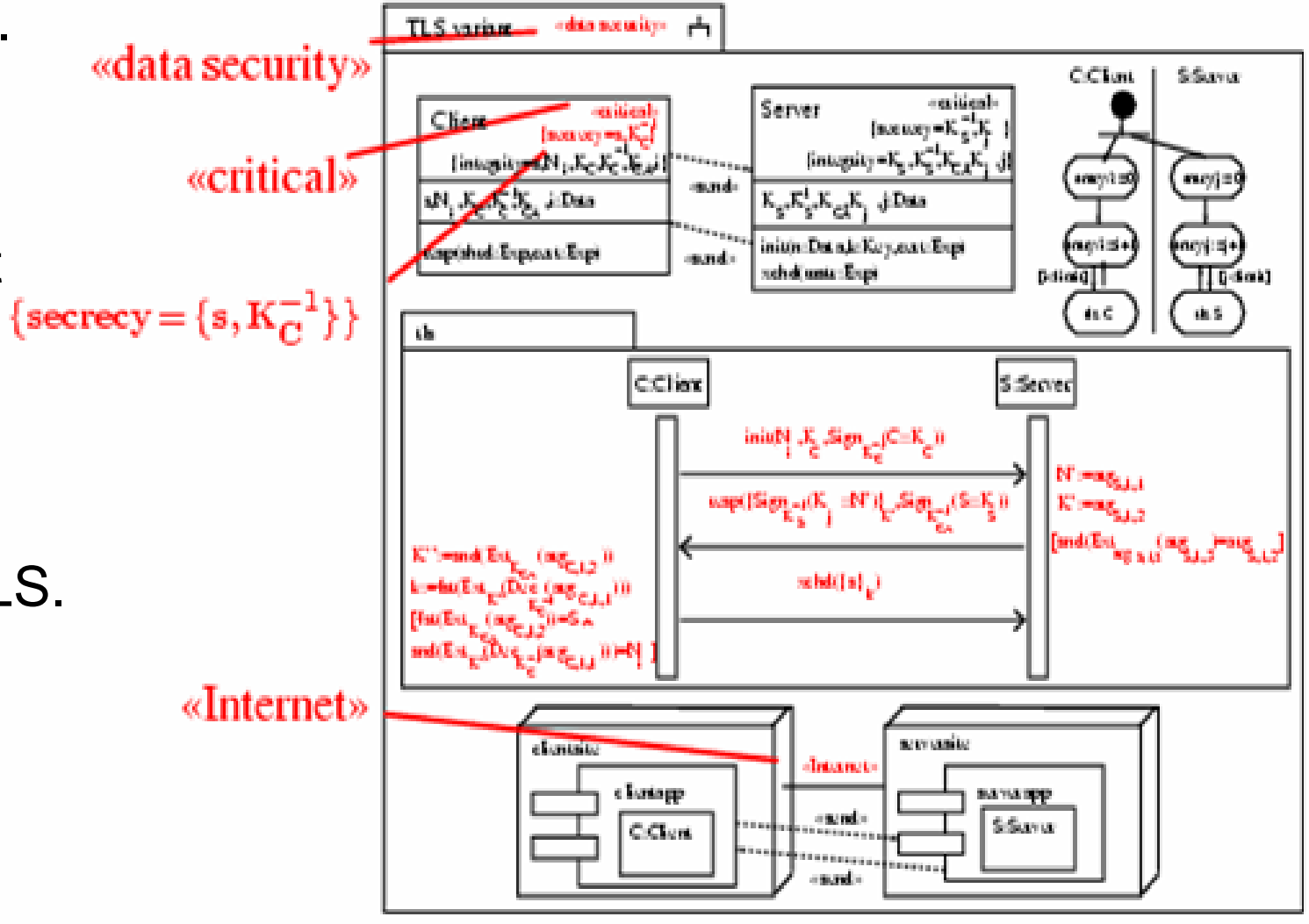
k^{-1}, y, x
$\{z\}_k$, z

Beispiel: Variante von TLS (SSL)

IEEE Infocom 1999.

Ziel:

- Vertrauliche Daten verschlüsselt unter Sitzungsschlüssel.
- Weniger Server-belastung als bei TLS.

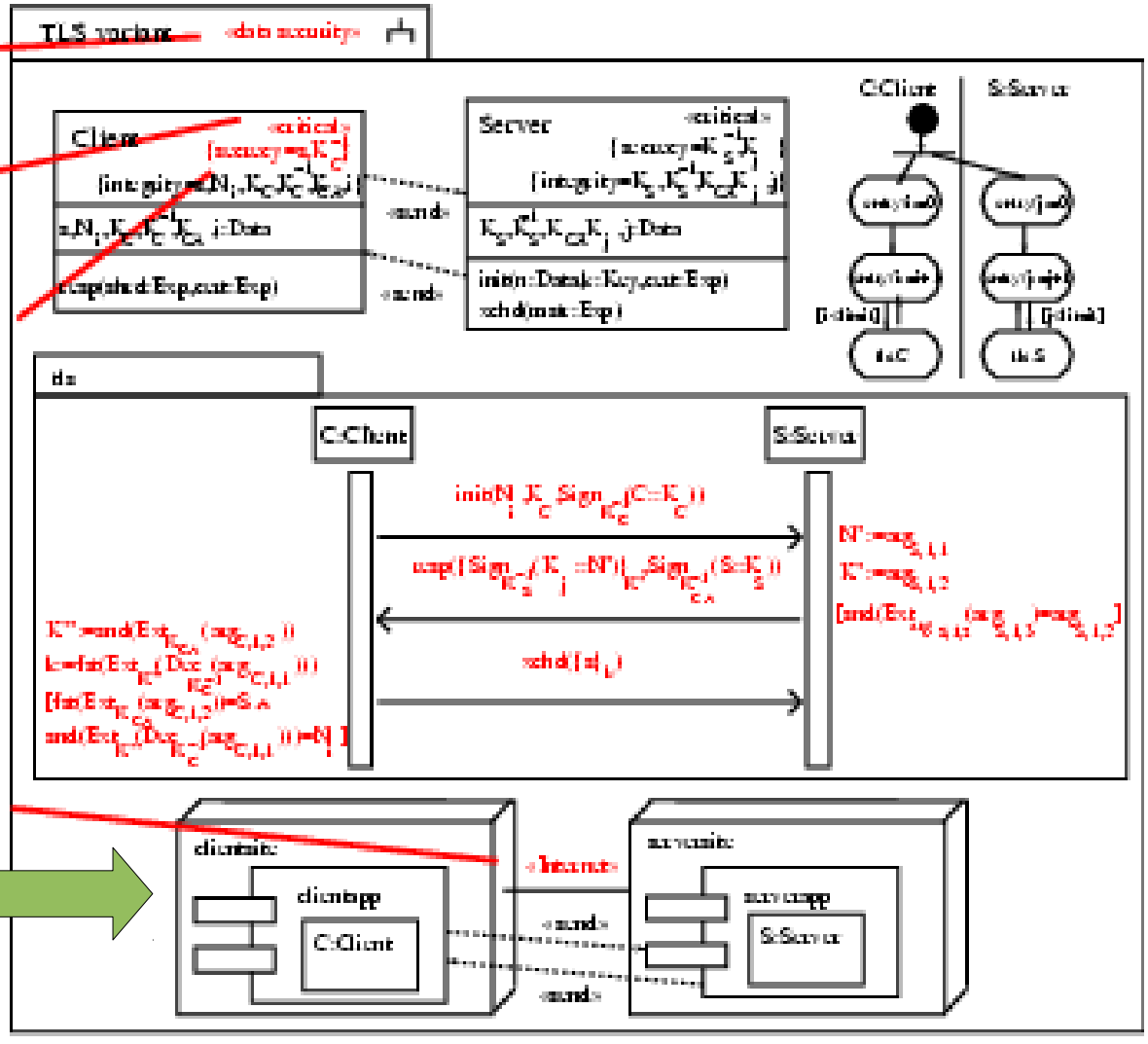


Beispiel: Variante von TLS

«data security»

«critical»

{secrecy = {s, K_C^{-1}}}



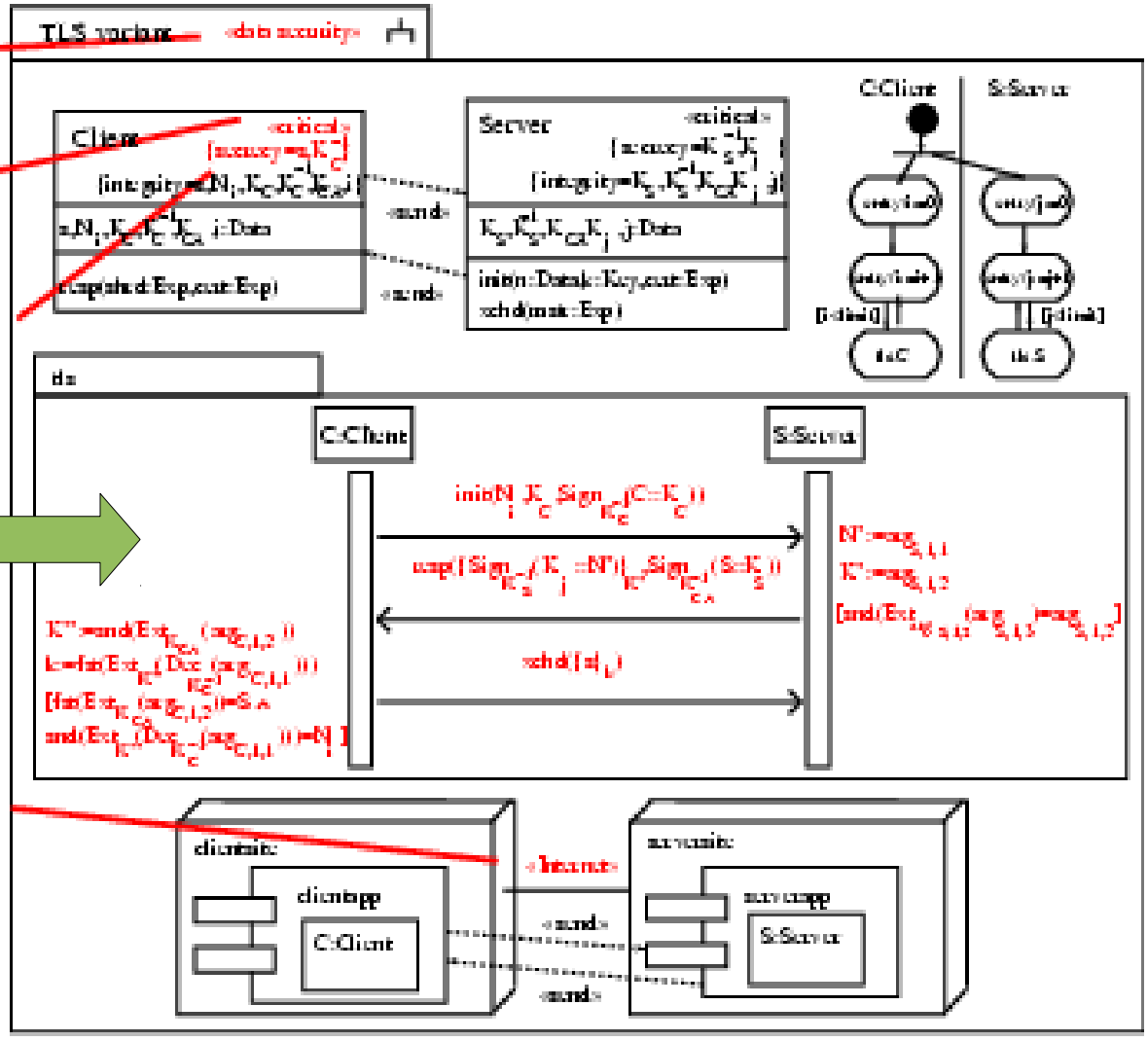
Verteilungsdiagram:
- Information über Nachrichten-verbindung
- Hier: Kommunikation über internet
- Standardangreifer kann diese Aktionen durchführen:

$Threats_{default}$(Internet) ∈ {delete, read,insert,access}

Variant of TLS (INFOCOM`99)

Beispiel: Variante von TLS

Sequenzdiagramm:
- Nachrichten zwischen verschiedenen Objekten/Komponenten senden
- Beinhaltet kryptographische Ausdrücke
- Z.B. xchd($\{s_i\}_k$)

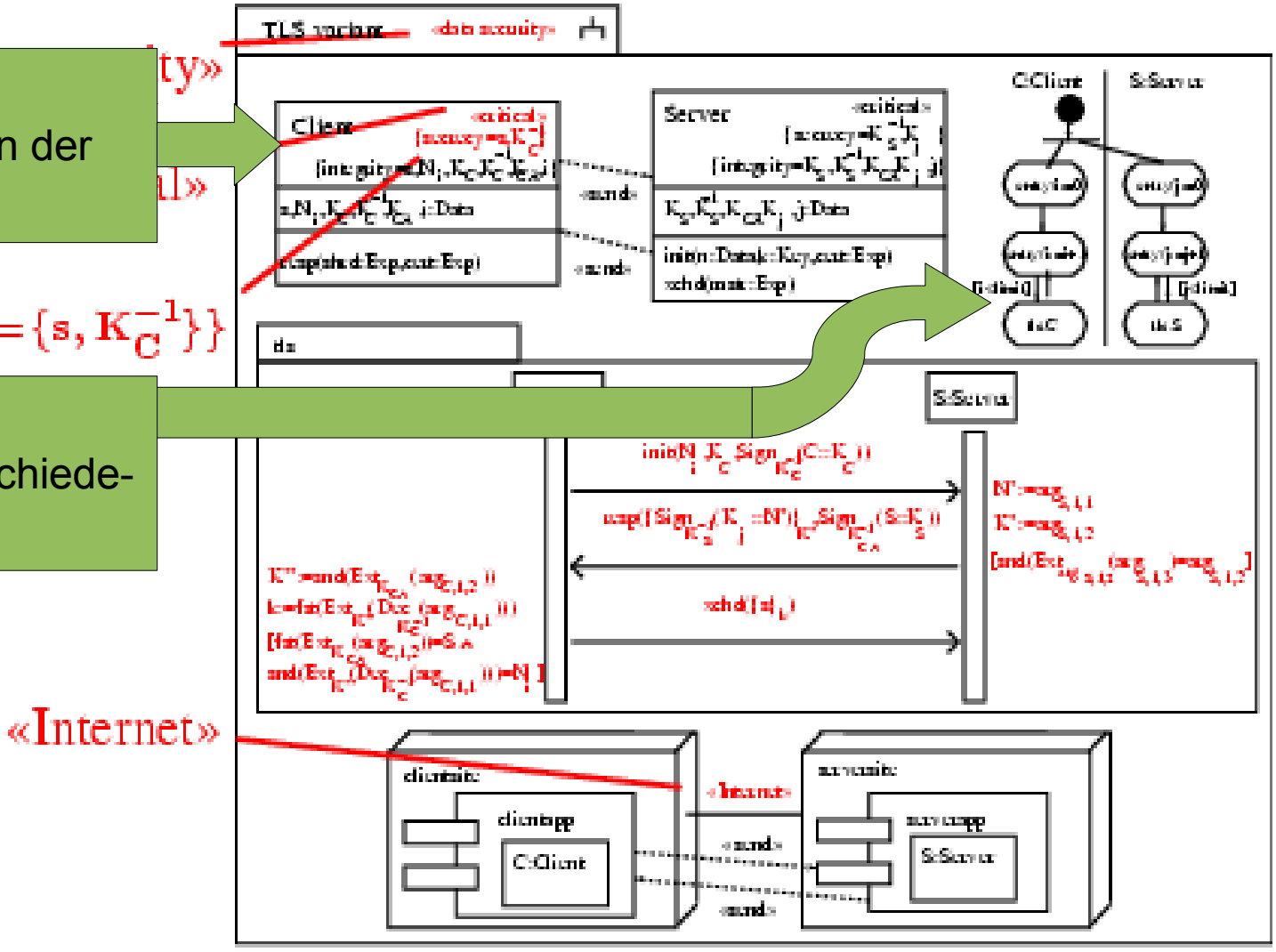


Variant of TLS (INFOCOM`99)

Beispiel: Variante von TLS

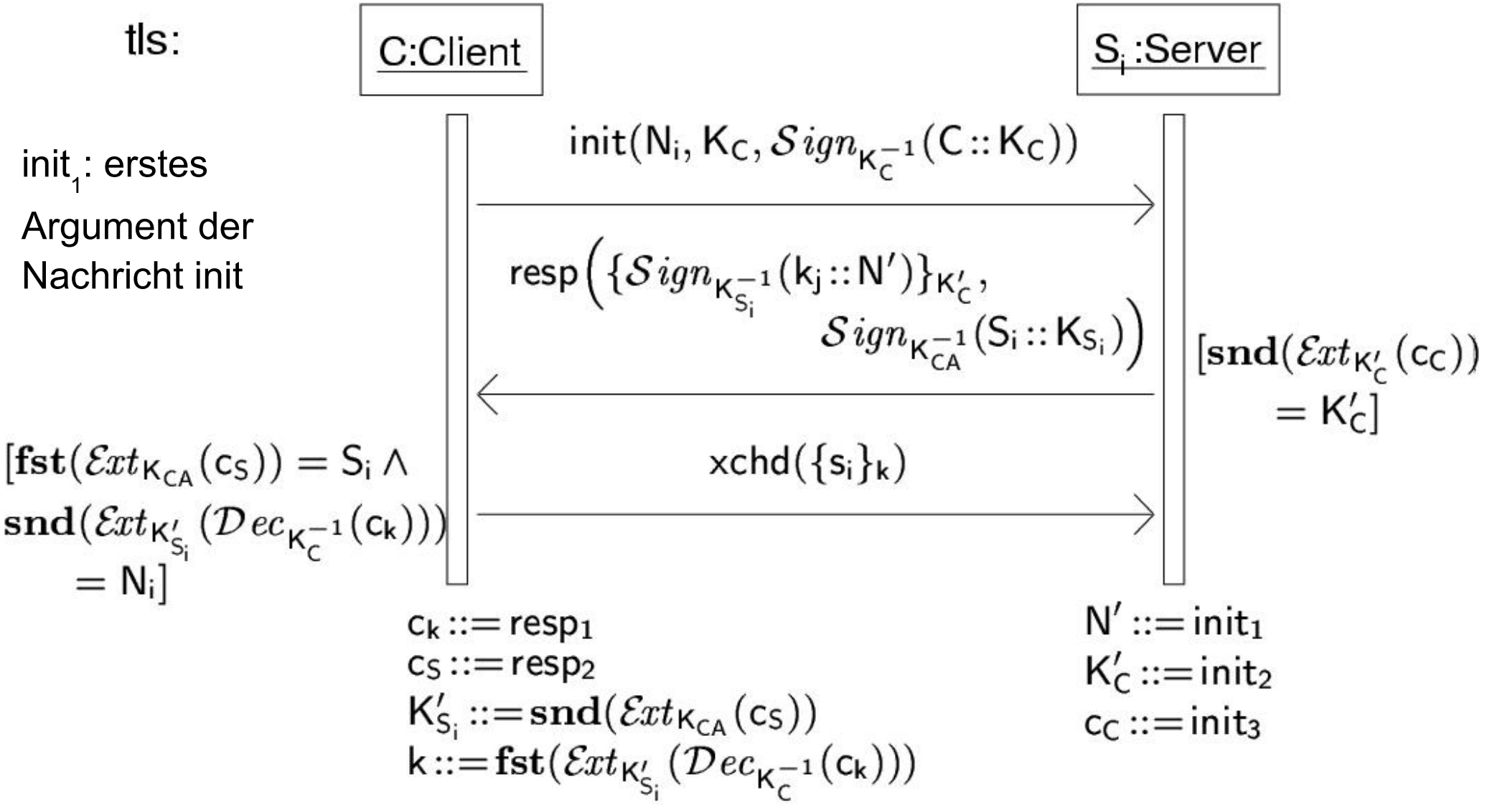
Klassendiagramm:
- Information über Variablen der Daten und Operationen

Aktivitätsdiagramm:
- Koordiniert Aktivitäten verschiedener Objekte/Komponente



Variant of TLS (INFOCOM`99)

Protokollablauf



Frage

- Annahme: Angreifer besitzt zum Schlüssel K_{CA} gehörenden vertraulichen Signaturschlüssel der Certification Authority (CA).
- Wie kommt er damit an zu übertragendes Geheimnis s_i ?

Zusammenfassung

- ISO Schichtenmodell und Sicherheit
- Angreifer-Modell
- Kryptographische Ausdrücke
- Kryptographische Protokolle