



# Symmetrische Verfahren III

Secure Sockets Layer -  
SSL

Transport Layer Security -  
TLS

Christoph Scheffel  
Christian – Weise – Gymnasium Zittau

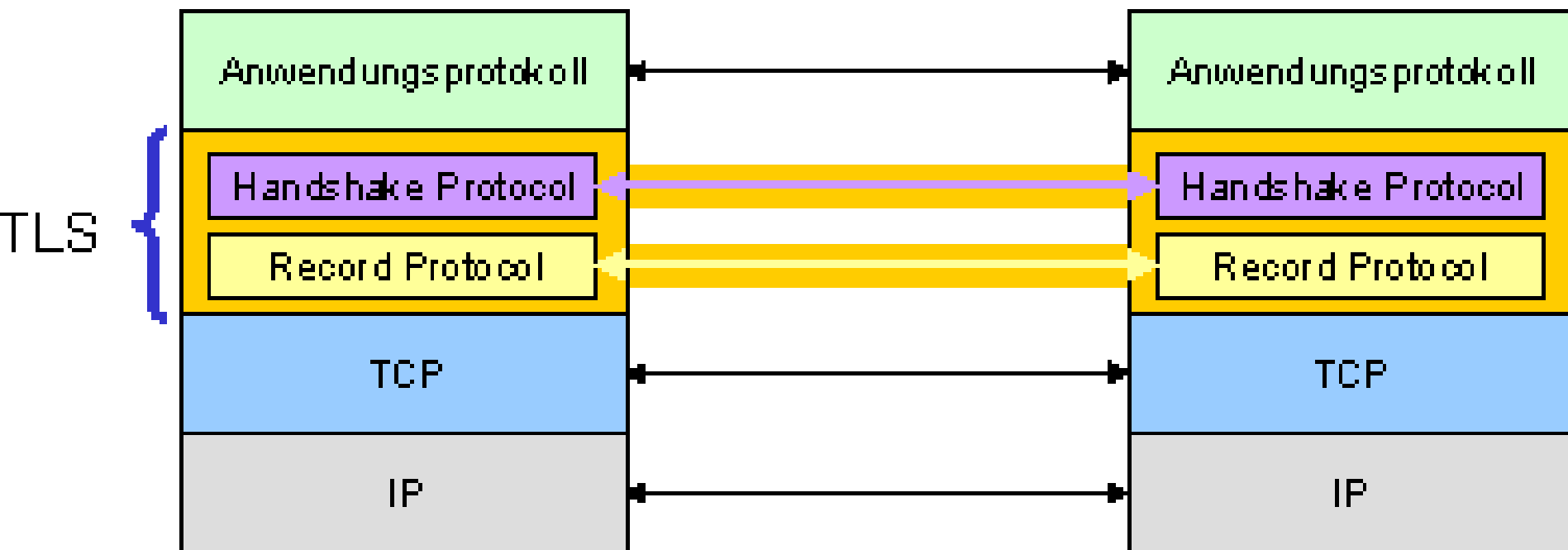
# [Gliederung]

1. Allgemeines
2. Funktionsweise
  1. Record Protocol
  2. Handshake Protocol
    1. Phase 1
    2. Phase 2
    3. Phase 3
    4. Phase 4
  3. Change Cipher Spec. Protocol
  4. Alert Protocol
  5. Application Data Protocol
3. Quellen

# [ 1. Allgemeines ]

- Hybrides Verschlüsselungsprogramm zu sicheren Datenübertragung im Internet
- im OSI-Schichtmodell in der Darstellungsschicht angeordnet
- Stellt sicher Verbindungen für Protokolle ohne eigene Sicherung zur Verfügung
- Erweiterbar, damit es zukunftssicher ist

# Position im Schichtenmodell



# [ 2. Funktionsweise ]

- Besteht aus zwei Schichten :

TSL Handshake Protocol	TSL Change Chipher Spec. Protocol	TSL Alert Protocol	TSL Aplication Data Protocol
TSL Record Protocol			

# [ 2.1. Record Protocol ]

- Zur Absicherung der Verbindung
- Zwei Dienste, die separat oder gemeinsam genutzt werden können:
  1. *Ende-zu-Ende- Verschlüsselung mittels symmetrischer Algorithmen*
  2. *Sicherung der Nachrichten-Integrität und Authentizität durch Bildung einer kryptografischen Prüfsumme (Hash-Funktion)*
- Fragmentierung der Daten und Zusammensetzen beim Empfänger
- Komprimieren der Daten → Aushandeln des kryptografischen Schlüssels mit dem TLS-Handshake Protocol

## 2.2. Handshake Protocol

- Baut auf dem Record Protocol auf
- Funktionen:
  1. *Identifikation und Authentifizierung der Kommunikationspartner*
  2. *Aushandeln zu benutzender kryptografischer Algorithmen und Schlüssel*
- „Handshake“ kann in 4 Phasen unterteilt werden

## 2.2.1. Phasen des Handshake Protocol - Phase 1

- Kontaktaufnahme zwischen Server und Client
- Wichtige Parameter:
  - Version
  - 32 Byte Zufallsinformation (Schutz vor Replay Attacken)
  - Session-ID (Erkennung von zusammenhängenden Anfragen eines Benutzers)
  - Die verwendeten Algorithmen

## 2.2.2. Phasen des Handshake Protocol - Phase 2

- Identifizierung des Servers gegenüber des Clients
- Übermittlung eines X.509v3-Zertifikats (Überprüfen der Authentizität bzw. Integrität)
- Server kann ein CertificateRequest an den Client schicken

## 2.2.3. Phasen des Handshake Protocol - Phase 3

- Client identifiziert sich gegenüber Server
- Client versucht Zertifikat zu verifizieren (bestätigen)
- Zertifikat enthält öffentlichen Schlüssel des Servers
- Gemeinsames pre-master-secret muss generiert werden

## 2.2.4. Phasen des Handshake Protocol - Phase 4

- Abschluss des „Handshake“
- Aus pre-master-secret wird das Master Secret (mit Hilfe einer spezifischen Pseudozufallsfunktion bzw. Hash-Funktion)
- Aus Master Secret wird einmaliger Sitzungsschlüssel („Session key“)
- Einmalig benutzbarer symmetrischer Schlüssel zum Ver- und Entschlüsseln der Daten
- Daten werden nur noch verschlüsselt verschickt

public key client



private key client

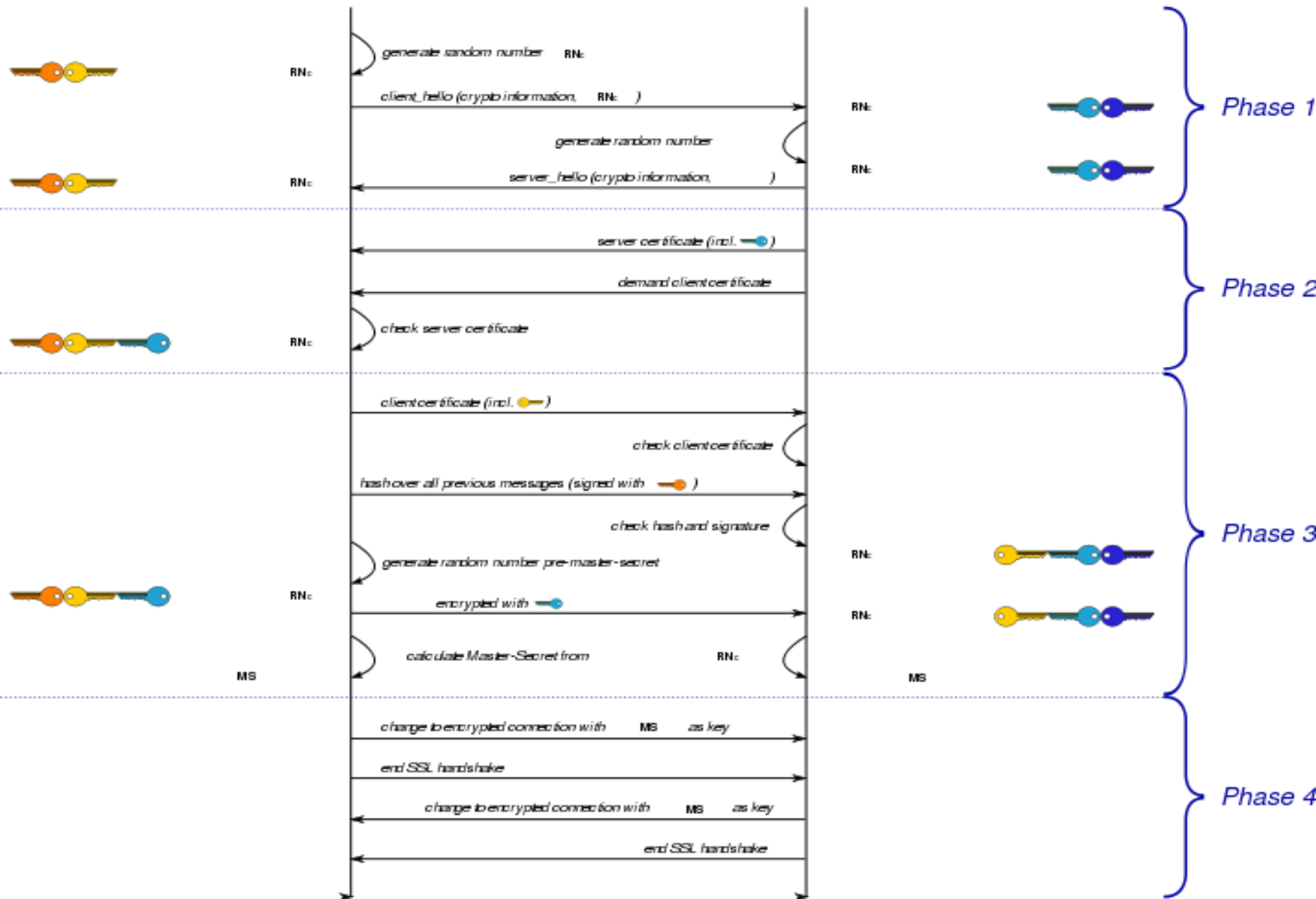


Client

Server

public key server

private key server



## 2.3. TLS Change Cipher Spec Protocoll

- Besteht nur aus einer einzigen Nachricht
- Sender teilt Empfänger mit dass in der aktiven Sitzung auf Cipher Suite gewechselt wird
- Cipher Suite wurde im Handshake Protocol ausgehandelt
- Cipher Suite legt fest welche Algorithmen beim Datenaustausch verwendet werden

## 2.4. TLS Alert Protocol

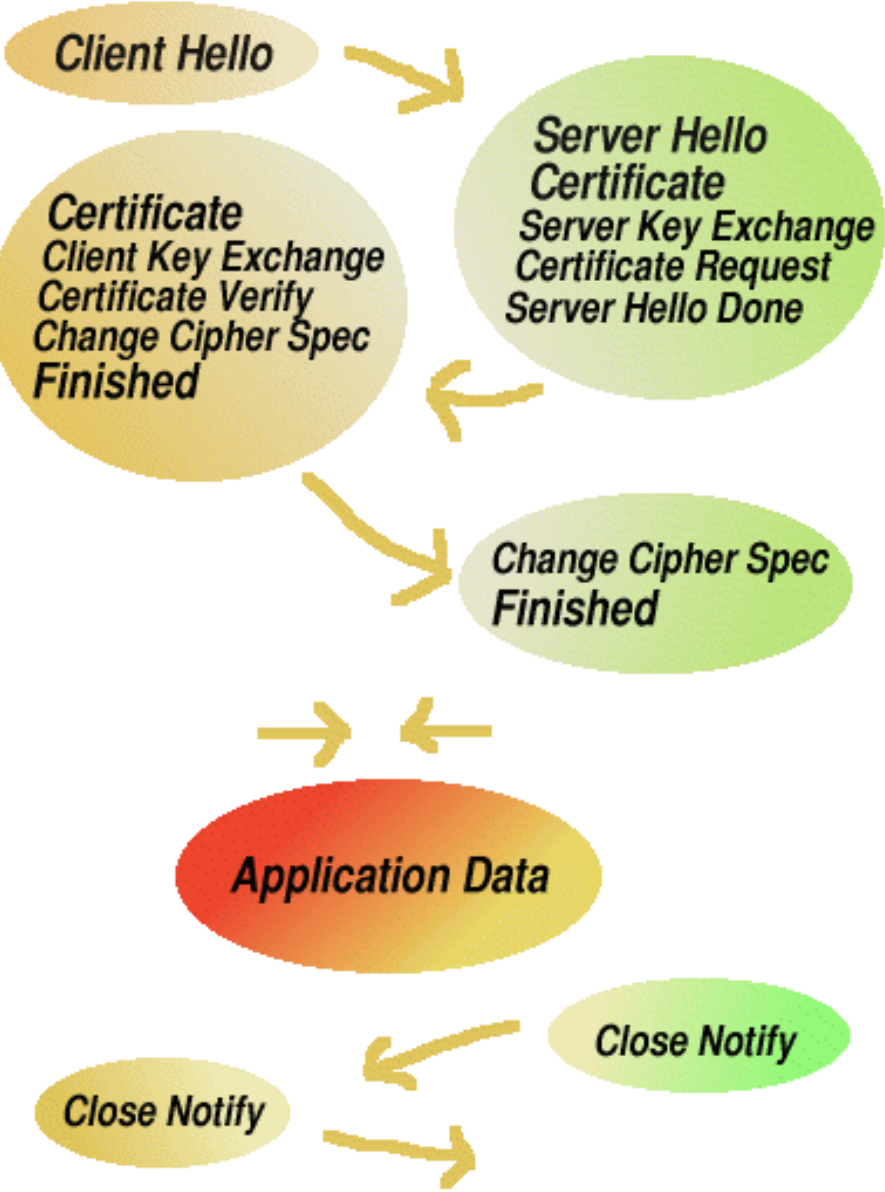
- Unterscheidet zwischen zwei dutzend verschiedenen Nachrichten
- z.B. Fehlermeldungen bzw. Warnungen
- Teilt auch den Abschluss des Verbindungsaufbaus mit

## 2.5. TSL Application Data Protocol

- Anwendungsdaten werden:
  - In Teile zerlegt
  - Komprimiert
  - Gegen Verfälschung geschützt
  - Je nach Stand der Sitzung auch verschlüsselt
- Keine inhaltliche Interpretation

**Client**

**Server**



# [ 3. Quellen ]

## Inhalt:

- [http://de.wikipedia.org/wiki/Transport\\_Layer\\_Security](http://de.wikipedia.org/wiki/Transport_Layer_Security); Stand: 30.09.11
- <http://de.wikipedia.org/wiki/X.509>; Stand: 06.11.11
- [http://de.wikipedia.org/wiki/Digitales\\_Zertifikat](http://de.wikipedia.org/wiki/Digitales_Zertifikat); Stand: 06.11.11
- <http://www.teialehrbuch.de/Kostenlose-Kurse/Internet-Technik/16263-TLS-Transport-Layer-Security.html>; Stand: 06.11.11
- [http://de.wikipedia.org/wiki/Cipher\\_Suite](http://de.wikipedia.org/wiki/Cipher_Suite); Stand: 06.11.1
- [http://www.repges.net/SSL/Architektur\\_SSL/Application\\_Data/application\\_data.html](http://www.repges.net/SSL/Architektur_SSL/Application_Data/application_data.html); Stand: 06.11.11

## Grafiken:

- [http://de.wikipedia.org/w/index.php?title=Datei:SSL\\_handshake\\_with\\_two\\_way\\_authentication\\_with\\_certificates.svg&filetimestamp=20100120123823](http://de.wikipedia.org/w/index.php?title=Datei:SSL_handshake_with_two_way_authentication_with_certificates.svg&filetimestamp=20100120123823); Stand: 06.11.11
- [http://www-ivs.cs.uni-magdeburg.de/~dumke/ProSem/tls\\_img/handshake.gif](http://www-ivs.cs.uni-magdeburg.de/~dumke/ProSem/tls_img/handshake.gif); Stand: 06.11.11
- <http://www.teialehrbuch.de/Kostenlose-Kurse/Internet-Technik/pics/LE10-tls-stack.png>; Stand: 06.11.11