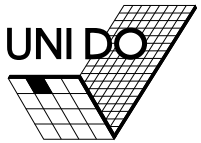
SSL-Protokoll und Internet-Sicherheit

Christina Bräutigam

Universität Dortmund

5. Dezember 2005



Übersicht

Übersicht

Übersicht

Übersicht

Übersicht

Übersicht

Einleitung

- Internet
  - Entstand zu Beginn der 80er Jahre des 20. Jahrhunderts
  - Anfangs ein Zusammenschluß von Computernetzen einiger Forschungsinstitute
- Mechanismen zur Sicherstellung von Datenauthentizität und -integrität notwendig
- Sicherheitssysteme für einzelne Dienste
  - IPSec (IP Security Protocol)
  - PGP (Pretty Good Privacy)
  - SSL (Secure Sockets Layer)

Einleitung

- Internet
  - Entstand zu Beginn der 80er Jahre des 20. Jahrhunderts
  - Anfangs ein Zusammenschluß von Computernetzen einiger Forschungsinstitute
- Mechanismen zur Sicherstellung von Datenauthentizität und -integrität notwendig
- Sicherheitssysteme für einzelne Dienste
  - IPSec (IP Security Protocol)
  - PGP (Pretty Good Privacy)
  - SSL (Secure Sockets Layer)

Einleitung

- Internet
  - Entstand zu Beginn der 80er Jahre des 20. Jahrhunderts
  - Anfangs ein Zusammenschluß von Computernetzen einiger Forschungsinstitute
- Mechanismen zur Sicherstellung von Datenauthentizität und -integrität notwendig
- Sicherheitssysteme für einzelne Dienste
  - IPSec (IP Security Protocol)
  - PGP (Pretty Good Privacy)
  - SSL (Secure Sockets Layer)

Einleitung

- Internet
  - Entstand zu Beginn der 80er Jahre des 20. Jahrhunderts
  - Anfangs ein Zusammenschluß von Computernetzen einiger Forschungsinstitute
- Mechanismen zur Sicherstellung von Datenauthentizität und -integrität notwendig
- Sicherheitssysteme für einzelne Dienste
  - IPSec (IP Security Protocol)
  - PGP (Pretty Good Privacy)
  - SSL (Secure Sockets Layer)

Einleitung

- Internet
  - Entstand zu Beginn der 80er Jahre des 20. Jahrhunderts
  - Anfangs ein Zusammenschluß von Computernetzen einiger Forschungsinstitute
- Mechanismen zur Sicherstellung von Datenauthentizität und -integrität notwendig
- Sicherheitssysteme für einzelne Dienste
  - IPSec (IP Security Protocol)
  - PGP (Pretty Good Privacy)
  - SSL (Secure Sockets Layer)

Einleitung

- Internet
  - Entstand zu Beginn der 80er Jahre des 20. Jahrhunderts
  - Anfangs ein Zusammenschluß von Computernetzen einiger Forschungsinstitute
- Mechanismen zur Sicherstellung von Datenauthentizität und -integrität notwendig
- Sicherheitssysteme für einzelne Dienste
  - IPSec (IP Security Protocol)
  - PGP (Pretty Good Privacy)
  - SSL (Secure Sockets Layer)

Einleitung

- Internet
  - Entstand zu Beginn der 80er Jahre des 20. Jahrhunderts
  - Anfangs ein Zusammenschluß von Computernetzen einiger Forschungsinstitute
- Mechanismen zur Sicherstellung von Datenauthentizität und -integrität notwendig
- Sicherheitssysteme für einzelne Dienste
  - IPSec (IP Security Protocol)
  - PGP (Pretty Good Privacy)
  - SSL (Secure Sockets Layer)

Einleitung

- Internet
  - Entstand zu Beginn der 80er Jahre des 20. Jahrhunderts
  - Anfangs ein Zusammenschluß von Computernetzen einiger Forschungsinstitute
- Mechanismen zur Sicherstellung von Datenauthentizität und -integrität notwendig
- Sicherheitssysteme für einzelne Dienste
  - IPSec (IP Security Protocol)
  - PGP (Pretty Good Privacy)
  - SSL (Secure Sockets Layer)

Allgemeines zu SSL

- Kriterien eines erfolgreichen Sicherheitsprotokolls
  - Serverseitige Kryptographie
  - Schliessen einer Sicherheitslücke
  - Anpassungsfähigkeit
- Ansatz von SSL:
  Einführung einer Sicherheitsschicht zwischen HTTP und TCP

Allgemeines zu SSL

- Kriterien eines erfolgreichen Sicherheitsprotokolls
  - Serverseitige Kryptographie
  - Schliessen einer Sicherheitslücke
  - Anpassungsfähigkeit
- Ansatz von SSL:
  Einführung einer Sicherheitsschicht zwischen HTTP und TCP

Allgemeines zu SSL

- Kriterien eines erfolgreichen Sicherheitsprotokolls
  - Serverseitige Kryptographie
  - Schliessen einer Sicherheitslücke
  - Anpassungsfähigkeit
- Ansatz von SSL:
  Einführung einer Sicherheitsschicht zwischen HTTP und TCP

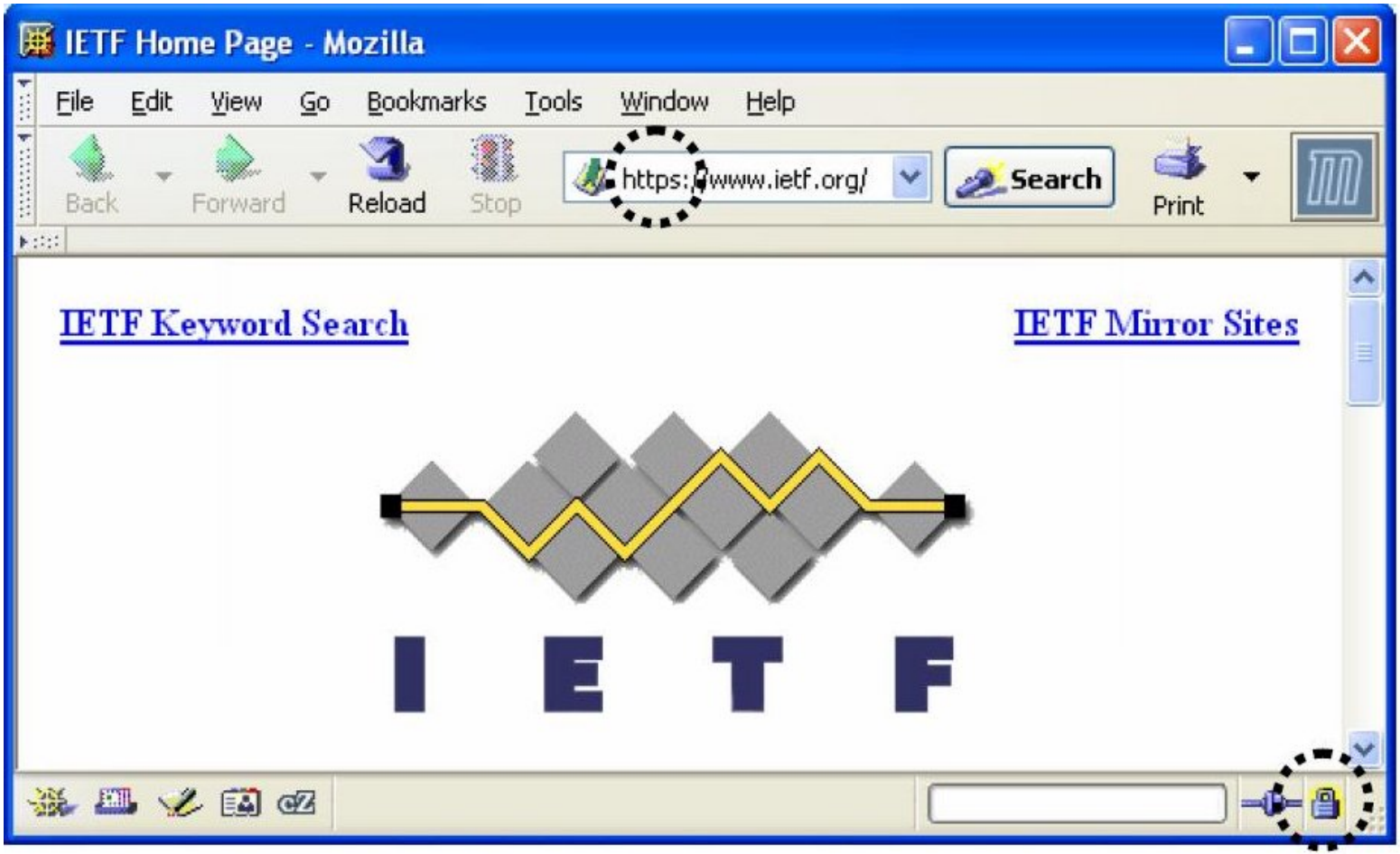
Allgemeines zu SSL

- Kriterien eines erfolgreichen Sicherheitsprotokolls
  - Serverseitige Kryptographie
  - Schliessen einer Sicherheitslücke
  - Anpassungsfähigkeit
- Ansatz von SSL:
  Einführung einer Sicherheitsschicht zwischen HTTP und TCP

Allgemeines zu SSL

- Kriterien eines erfolgreichen Sicherheitsprotokolls
  - Serverseitige Kryptographie
  - Schliessen einer Sicherheitslücke
  - Anpassungsfähigkeit
- Ansatz von SSL:
  Einführung einer Sicherheitsschicht zwischen HTTP und TCP

Allgemeines zu SSL



Ziele

- Vertraulichkeit der Daten mittels kryptographischer Verschlüsselungsverfahren
- Datenintegrität durch Hash-Funktionen
- Authentizität durch Zertifikate und digitale Signaturen

Ziele

- Vertraulichkeit der Daten mittels kryptographischer Verschlüsselungsverfahren
- Datenintegrität durch Hash-Funktionen
- Authentizität durch Zertifikate und digitale Signaturen

Ziele

- Vertraulichkeit der Daten mittels kryptographischer Verschlüsselungsverfahren
- Datenintegrität durch Hash-Funktionen
- Authentizität durch Zertifikate und digitale Signaturen

Geschichte

1993 Mosaic 1.0 des National Center for Supercomputing Applications (NCSA)

1994 Veröffentlichung von SSL 1.0 durch Netscape Communication

1995 Netcape Navigator, SSL 2.0

1996 Internet Explorer und PCT von Microsoft als Antwort auf SSL

1999 Festlegung von TLS (Transport Layer Security) als Standard durch IETF

Geschichte

1993 Mosaic 1.0 des National Center for Supercomputing Applications (NCSA)

1994 Veröffentlichung von SSL 1.0 durch Netscape Communication

1995 Netcape Navigator, SSL 2.0

1996 Internet Explorer und PCT von Microsoft als Antwort auf SSL

1999 Festlegung von TLS (Transport Layer Security) als Standard durch IETF

Geschichte

1993 Mosaic 1.0 des National Center for Supercomputing Applications (NCSA)

1994 Veröffentlichung von SSL 1.0 durch Netscape Communication

1995 Netcape Navigator, SSL 2.0

1996 Internet Explorer und PCT von Microsoft als Antwort auf SSL

1999 Festlegung von TLS (Transport Layer Security) als Standard durch IETF

Geschichte

1993 Mosaic 1.0 des National Center for Supercomputing Applications (NCSA)

1994 Veröffentlichung von SSL 1.0 durch Netscape Communication

1995 Netcape Navigator, SSL 2.0

1996 Internet Explorer und PCT von Microsoft als Antwort auf SSL

1999 Festlegung von TLS (Transport Layer Security) als Standard durch IETF

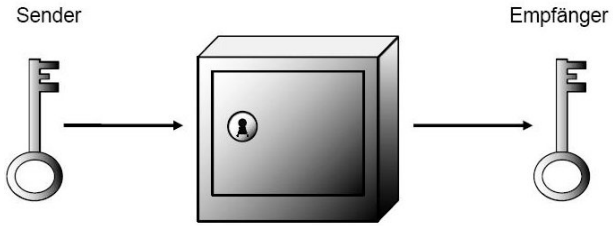
Geschichte

- 1993 Mosaic 1.0 des National Center for Supercomputing Applications (NCSA)
- 1994 Veröffentlichung von SSL 1.0 durch Netscape Communication
- 1995 Netcape Navigator, SSL 2.0
- 1996 Internet Explorer und PCT von Microsoft als Antwort auf SSL
- 1999 Festlegung von TLS (Transport Layer Security) als Standard durch IETF

Verwendete kryptographische Verfahren

Symmetrische Verschlüsselung

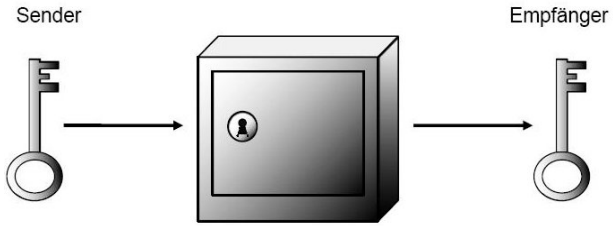
- Zur eigentlichen Datenverschlüsslung
- Problem: sicherer Austausch des gemeinsamen, geheimen Schlüssels
- Lösung: asymmetrische Verschlüsselung
- Beispiele: DES, IDEA



Verwendete kryptographische Verfahren

Symmetrische Verschlüsselung

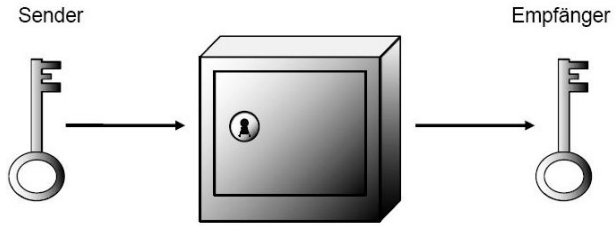
- Zur eigentlichen Datenverschlüsslung
- Problem: sicherer Austausch des gemeinsamen, geheimen Schlüssels
- Lösung: asymmetrische Verschlüsselung
- Beispiele: DES, IDEA



Verwendete kryptographische Verfahren

Symmetrische Verschlüsselung

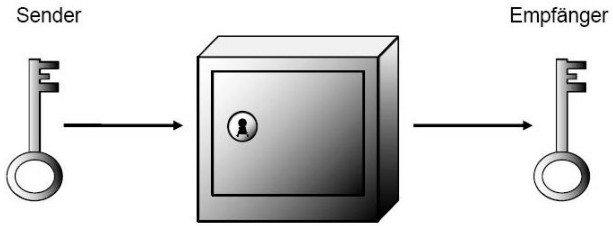
- Zur eigentlichen Datenverschlüsslung
- Problem: sicherer Austausch des gemeinsamen, geheimen Schlüssels
- Lösung: asymmetrische Verschlüsselung
- Beispiele: DES, IDEA



Verwendete kryptographische Verfahren

Symmetrische Verschlüsselung

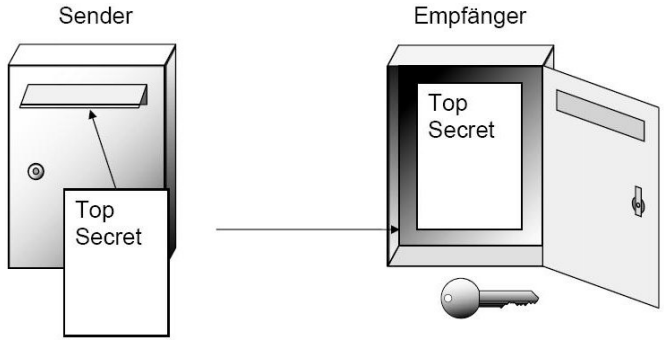
- Zur eigentlichen Datenverschlüsslung
- Problem: sicherer Austausch des gemeinsamen, geheimen Schlüssels
- Lösung: asymmetrische Verschlüsselung
- Beispiele: DES, IDEA



Verwendete kryptographische Verfahren

Asymmetrische Verschlüsselung

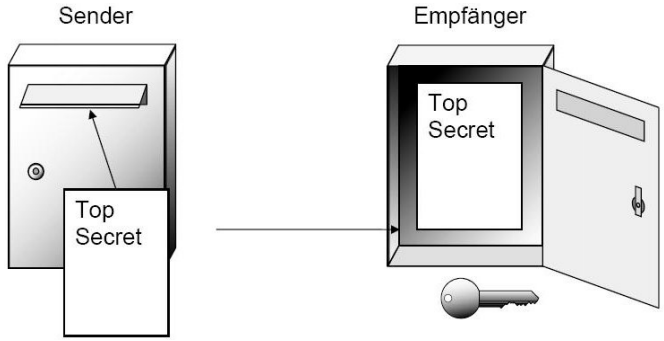
- Sender besitzt Schlüsselpaar (privateKey, publicKey)
- Verschlüsselung mit privateKey, Entschlüsselung nur durch publicKey durch Empfänger
- Bei Antwort: Verschlüsselung mit publicKey, Entschlüsselung durch privateKey
- Nachteil: keine Gewährleistung, dass publicKey vom Sender ist
- Lösung: Einsatz von Zertifikaten
- Beispiel: RSA



Verwendete kryptographische Verfahren

Asymmetrische Verschlüsselung

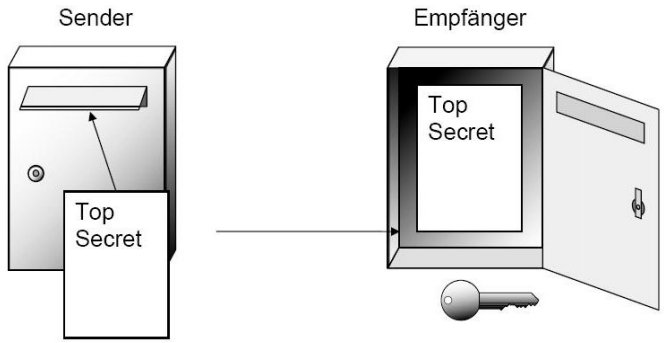
- Sender besitzt Schlüsselpaar (privateKey, publicKey)
- Verschlüsselung mit privateKey, Entschlüsselung nur durch publicKey durch Empfänger
- Bei Antwort: Verschlüsselung mit publicKey, Entschlüsselung durch privateKey
- Nachteil: keine Gewährleistung, dass publicKey vom Sender ist
- Lösung: Einsatz von Zertifikaten
- Beispiel: RSA



Verwendete kryptographische Verfahren

Asymmetrische Verschlüsselung

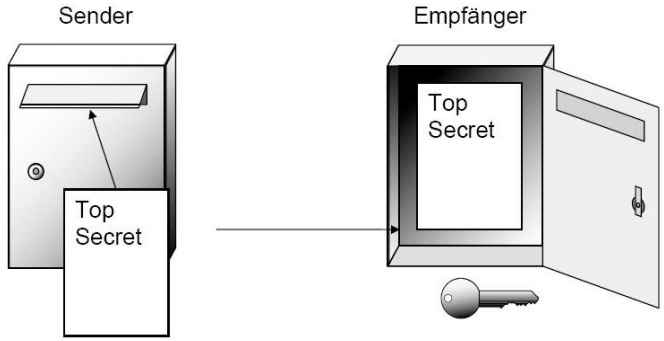
- Sender besitzt Schlüsselpaar (privateKey, publicKey)
- Verschlüsselung mit privateKey, Entschlüsselung nur durch publicKey durch Empfänger
- Bei Antwort: Verschlüsselung mit publicKey, Entschlüsselung durch privateKey
- Nachteil: keine Gewährleistung, dass publicKey vom Sender ist
- Lösung: Einsatz von Zertifikaten
- Beispiel: RSA



Verwendete kryptographische Verfahren

Asymmetrische Verschlüsselung

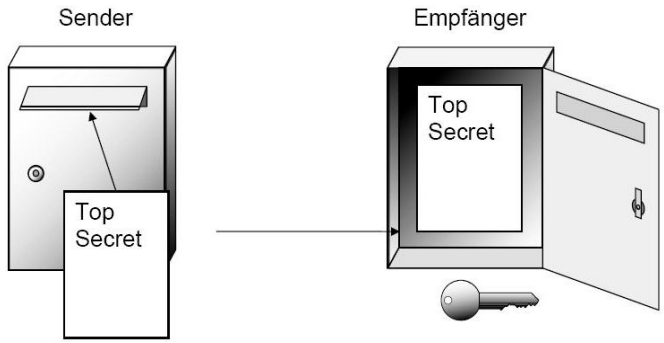
- Sender besitzt Schlüsselpaar (privateKey, publicKey)
- Verschlüsselung mit privateKey, Entschlüsselung nur durch publicKey durch Empfänger
- Bei Antwort: Verschlüsselung mit publicKey, Entschlüsselung durch privateKey
- Nachteil: keine Gewährleistung, dass publicKey vom Sender ist
- Lösung: Einsatz von Zertifikaten
- Beispiel: RSA



Verwendete kryptographische Verfahren

Asymmetrische Verschlüsselung

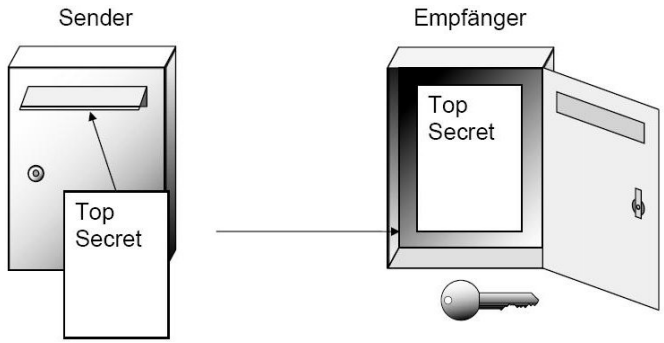
- Sender besitzt Schlüsselpaar (privateKey, publicKey)
- Verschlüsselung mit privateKey, Entschlüsselung nur durch publicKey durch Empfänger
- Bei Antwort: Verschlüsselung mit publicKey, Entschlüsselung durch privateKey
- Nachteil: keine Gewährleistung, dass publicKey vom Sender ist
- Lösung: Einsatz von Zertifikaten
- Beispiel: RSA



Verwendete kryptographische Verfahren

Asymmetrische Verschlüsselung

- Sender besitzt Schlüsselpaar (privateKey, publicKey)
- Verschlüsselung mit privateKey, Entschlüsselung nur durch publicKey durch Empfänger
- Bei Antwort: Verschlüsselung mit publicKey, Entschlüsselung durch privateKey
- Nachteil: keine Gewährleistung, dass publicKey vom Sender ist
- Lösung: Einsatz von Zertifikaten
- Beispiel: RSA



Verwendete kryptographische Verfahren

Hash-Funktionen

- Kryptographische Prüfsumme (Fingerabdruck)
- Zur Authentifizierung und Sicherstellung der Datenintegrität
- MAC (Message Authentication Code)
  Chiffre des Fingerabdrucks mit geheimen Schlüssel
- Beispiele: MD5, SHA-1

Verwendete kryptographische Verfahren

Hash-Funktionen

- Kryptographische Prüfsumme (Fingerabdruck)
- Zur Authentifizierung und Sicherstellung der Datenintegrität
- MAC (Message Authentication Code)
  Chiffre des Fingerabdrucks mit geheimen Schlüssel
- Beispiele: MD5, SHA-1

Verwendete kryptographische Verfahren

Hash-Funktionen

- Kryptographische Prüfsumme (Fingerabdruck)
- Zur Authentifizierung und Sicherstellung der Datenintegrität
- MAC (Message Authentication Code)
  Chiffre des Fingerabdrucks mit geheimen Schlüssel
- Beispiele: MD5, SHA-1

Verwendete kryptographische Verfahren

Hash-Funktionen

- Kryptographische Prüfsumme (Fingerabdruck)
- Zur Authentifizierung und Sicherstellung der Datenintegrität
- MAC (Message Authentication Code)
  Chiffre des Fingerabdrucks mit geheimen Schlüssel
- Beispiele: MD5, SHA-1

Verwendete kryptographische Verfahren

Digitale Signatur

- Nachweis der Sender-Authentizität und der Nachrichten-Integrität
- Signatur des Nachrichten-Hashwertes mit privateKey
- Überprüfung mit publicKey des Senders

Verwendete kryptographische Verfahren

Digitale Signatur

- Nachweis der Sender-Authentizität und der Nachrichten-Integrität
- Signatur des Nachrichten-Hashwertes mit privateKey
- Überprüfung mit publicKey des Senders

Verwendete kryptographische Verfahren

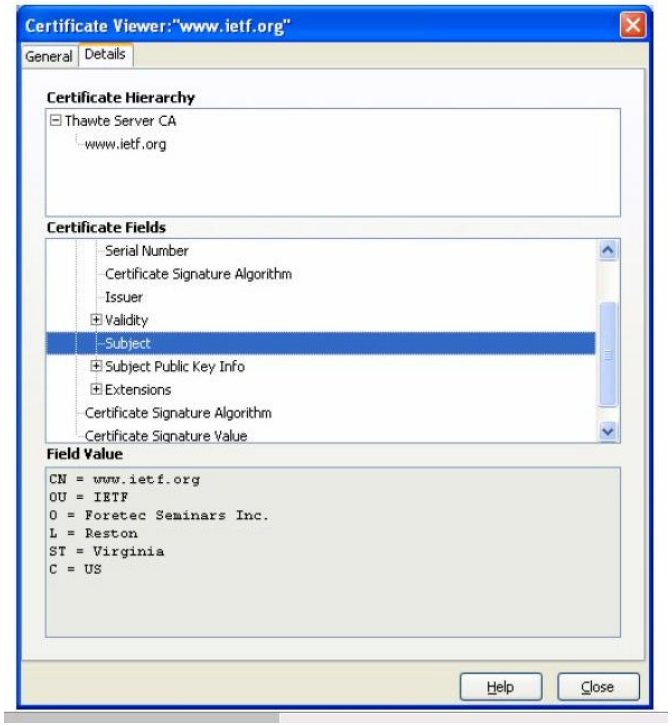
Digitale Signatur

- Nachweis der Sender-Authentizität und der Nachrichten-Integrität
- Signatur des Nachrichten-Hashwertes mit privateKey
- Überprüfung mit publicKey des Senders

Verwendete kryptographische Verfahren

Zertifikate

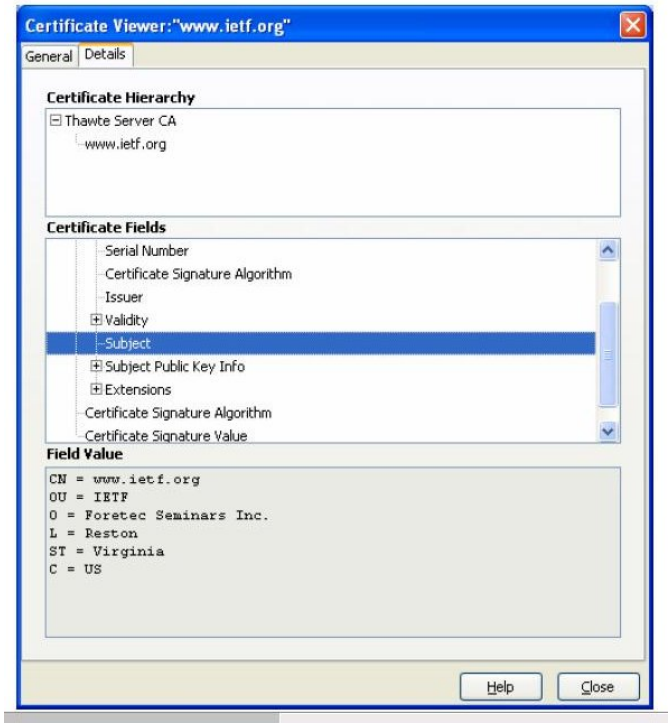
- Eindeutige Zuordnung eines publicKeys zu einer Person/Institution
- Zertifizierungshierarchie
- SSL-Zertifikat



Verwendete kryptographische Verfahren

Zertifikate

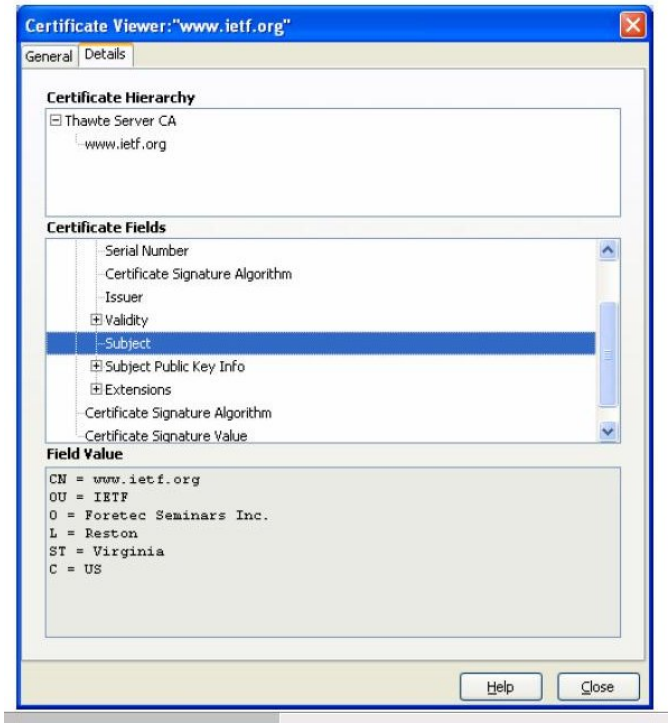
- Eindeutige Zuordnung eines publicKeys zu einer Person/Institution
- Zertifizierungshierarchie
- SSL-Zertifikat



Verwendete kryptographische Verfahren

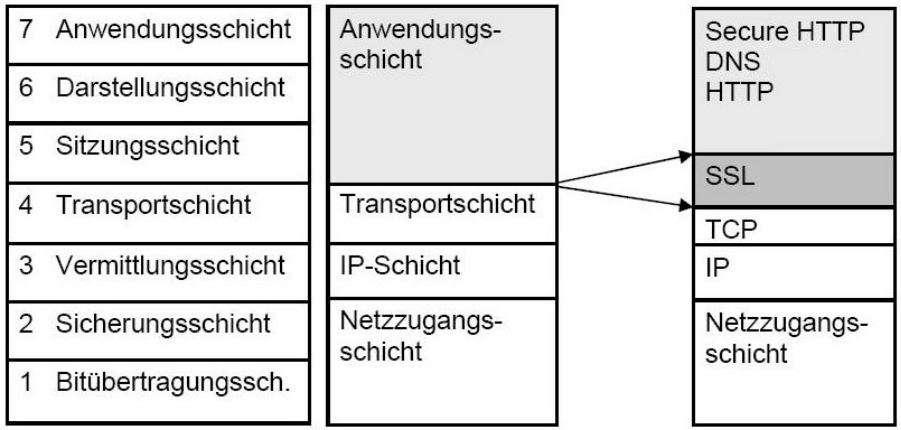
Zertifikate

- Eindeutige Zuordnung eines publicKeys zu einer Person/Institution
- Zertifizierungshierarchie
- SSL-Zertifikat



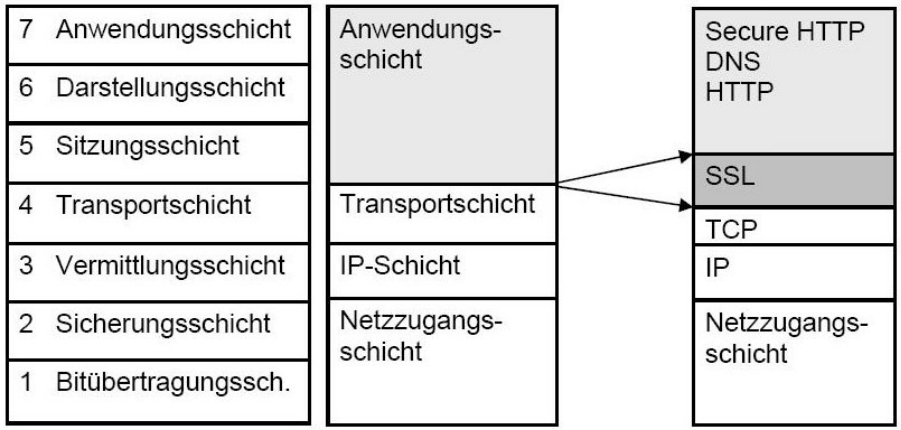
Hypertext Transfer Protokoll (HTTP)

- Basis für WWW: Hypertext Transfer Protokoll (HTTP) Hypertext Markup Language(HTML)
- HTTP nutzt TCP, das auf IP aufsetzt
- Absicherung der Socket Verbindung durch SSL
- SSL,PCT, TLS: Aufbau eines sicheren Kanals oberhalb TCP-Verbindung



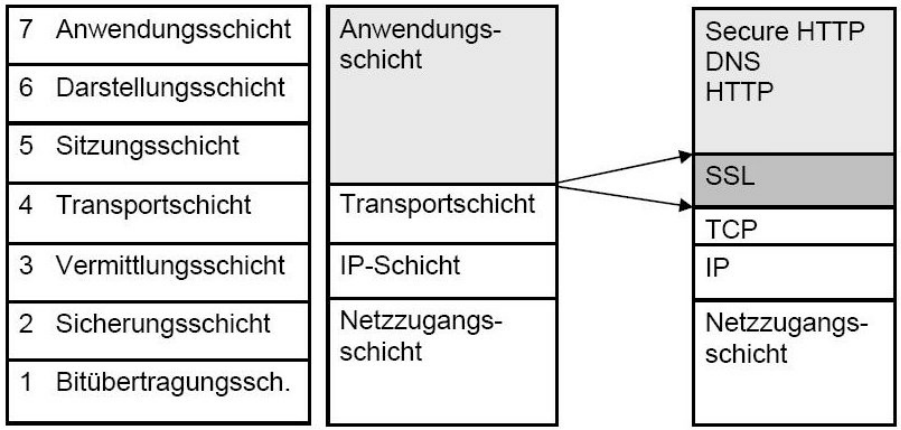
Hypertext Transfer Protokoll (HTTP)

- Basis für WWW: Hypertext Transfer Protokoll (HTTP) Hypertext Markup Language(HTML)
- HTTP nutzt TCP, das auf IP aufsetzt
- Absicherung der Socket Verbindung durch SSL
- SSL,PCT, TLS: Aufbau eines sicheren Kanals oberhalb TCP-Verbindung



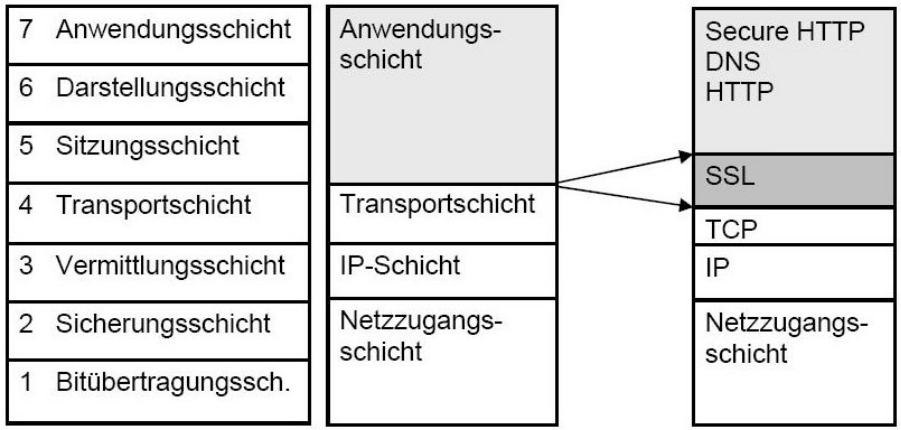
Hypertext Transfer Protokoll (HTTP)

- Basis für WWW: Hypertext Transfer Protokoll (HTTP) Hypertext Markup Language(HTML)
- HTTP nutzt TCP, das auf IP aufsetzt
- Absicherung der Socket Verbindung durch SSL
- SSL,PCT, TLS: Aufbau eines sicheren Kanals oberhalb TCP-Verbindung



Hypertext Transfer Protokoll (HTTP)

- Basis für WWW: Hypertext Transfer Protokoll (HTTP) Hypertext Markup Language(HTML)
- HTTP nutzt TCP, das auf IP aufsetzt
- Absicherung der Socket Verbindung durch SSL
- SSL,PCT, TLS: Aufbau eines sicheren Kanals oberhalb TCP-Verbindung



HTTP-Schutzmechanismen

- “Basic Authentication“ Methode
- “Digest Access Authentication“ Methode
- Secure HTTP (s-HTTP)

HTTP-Schutzmechanismen

- “Basic Authentication“ Methode
- “Digest Access Authentication“ Methode
- Secure HTTP (s-HTTP)

HTTP-Schutzmechanismen

- “Basic Authentication“ Methode
- “Digest Access Authentication“ Methode
- Secure HTTP (s-HTTP)

Wiederholung: Sicherheitsziele

- Vertraulichkeit
- Authentifikation der Kommunikationspartner
- Integrität
- Keine Gewährleistung der Verbindlichkeiten der Nachrichten

Wiederholung: Sicherheitsziele

- Vertraulichkeit
- Authentifikation der Kommunikationspartner
- Integrität
- Keine Gewährleistung der Verbindlichkeiten der Nachrichten

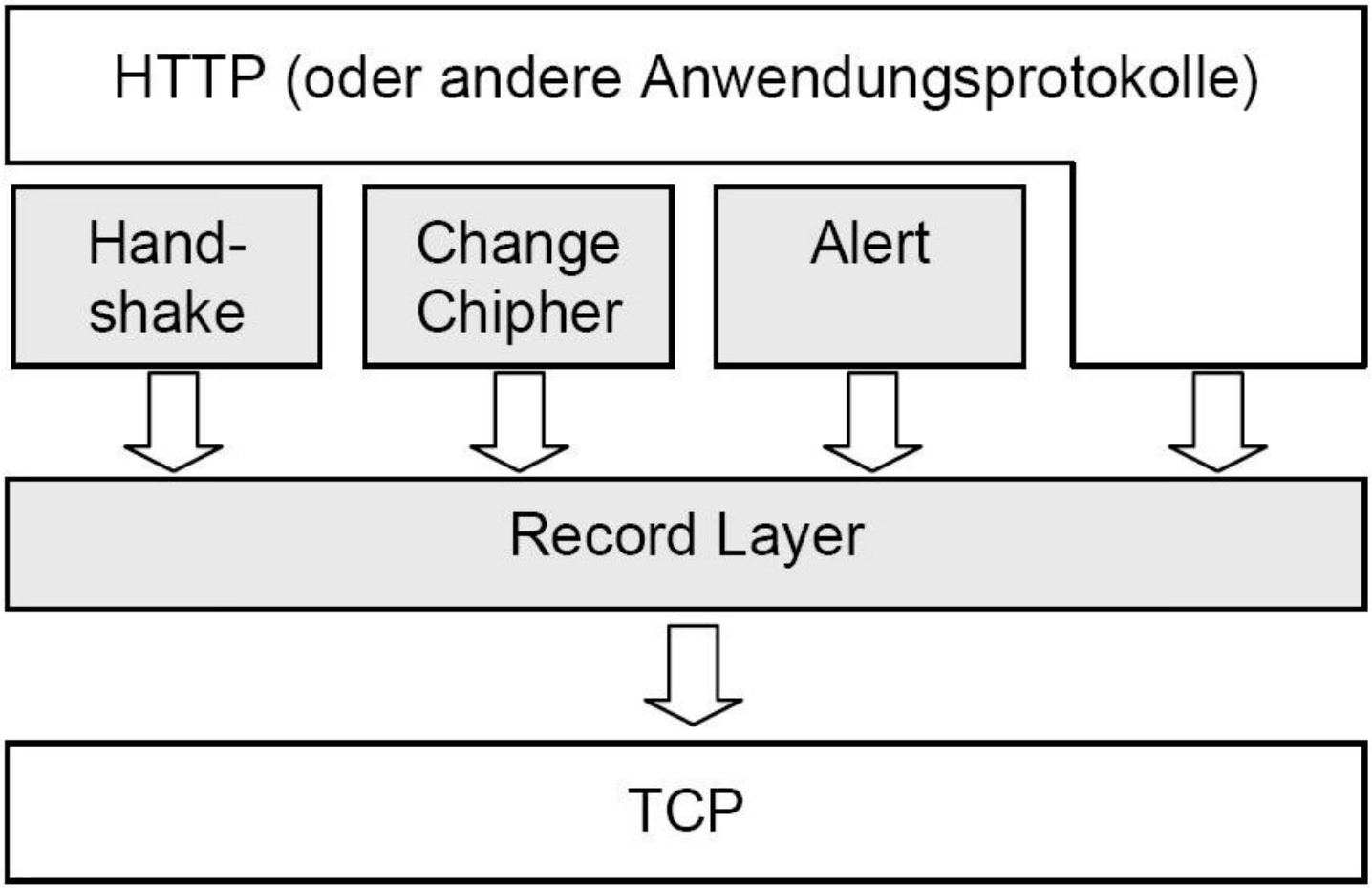
Wiederholung: Sicherheitsziele

- Vertraulichkeit
- Authentifikation der Kommunikationspartner
- Integrität
- Keine Gewährleistung der Verbindlichkeiten der Nachrichten

Wiederholung: Sicherheitsziele

- Vertraulichkeit
- Authentifikation der Kommunikationspartner
- Integrität
- Keine Gewährleistung der Verbindlichkeiten der Nachrichten

Bestandteile von SSL 3.0



SSL Handshake

2 Wege Austausch auf Basis eines Public Key Verschlüsselungsverfahren:

- Server sendet in SSL-Zertifikat verpackten öffentlichen Schlüssel an Client
- Client verschlüsselt geheime Zufallszahl mit öffentlichem Server-Schlüssel und sendet sie an Server
  Verwendung zur Berechnung der symmetrischen Schlüssel
- Realisierung durch Certificate und ClientKeyExchange
- Umrahmung dieses Austausches durch Absprache- und Synchronisationsnachrichten

SSL Handshake

2 Wege Austausch auf Basis eines Public Key Verschlüsselungsverfahren:

- Server sendet in SSL-Zertifikat verpackten öffentlichen Schlüssel an Client
- Client verschlüsselt geheime Zufallszahl mit öffentlichem Server-Schlüssel und sendet sie an Server
  Verwendung zur Berechnung der symmetrischen Schlüssel
- Realisierung durch Certificate und ClientKeyExchange
- Umrahmung dieses Austausches durch Absprache- und Synchronisationsnachrichten

SSL Handshake

2 Wege Austausch auf Basis eines Public Key Verschlüsselungsverfahren:

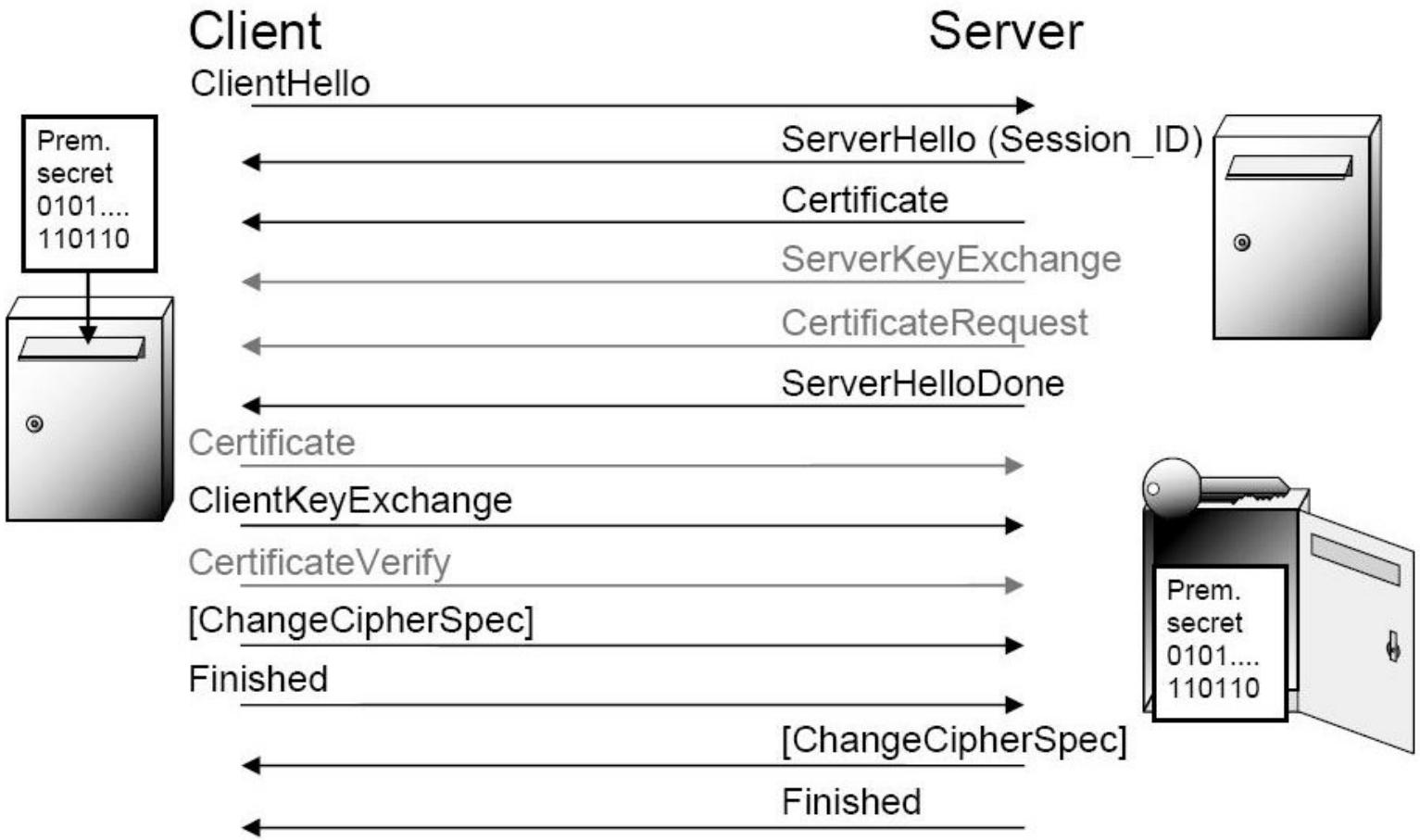
- Server sendet in SSL-Zertifikat verpackten öffentlichen Schlüssel an Client
- Client verschlüsselt geheime Zufallszahl mit öffentlichem Server-Schlüssel und sendet sie an Server
  Verwendung zur Berechnung der symmetrischen Schlüssel
- Realisierung durch Certificate und ClientKeyExchange
- Umrahmung dieses Austausches durch Absprache- und Synchronisationsnachrichten

SSL Handshake

2 Wege Austausch auf Basis eines Public Key Verschlüsselungsverfahren:

- Server sendet in SSL-Zertifikat verpackten öffentlichen Schlüssel an Client
- Client verschlüsselt geheime Zufallszahl mit öffentlichem Server-Schlüssel und sendet sie an Server
  Verwendung zur Berechnung der symmetrischen Schlüssel
- Realisierung durch Certificate und ClientKeyExchange
- Umrahmung dieses Austausches durch Absprache- und Synchronisationsnachrichten

SSL Handshake-Nachrichten



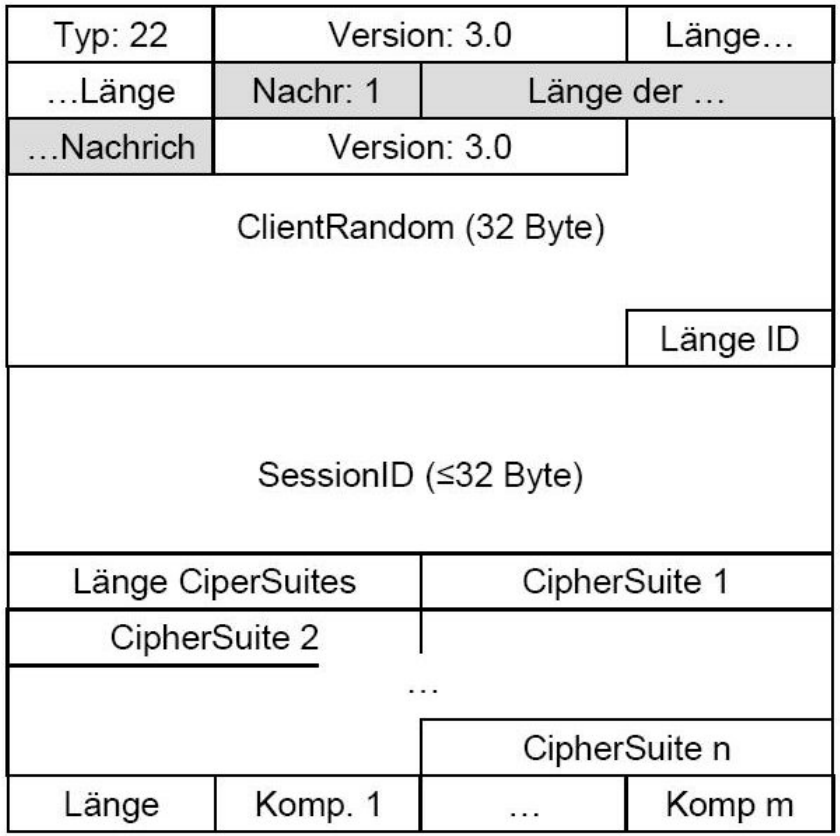
SSL Handshake-Nachrichten

ClientHello-Nachricht

- ProtocolVersion
- ClientRandom
- SessionID(optional)
- Ciphersuites

ServerHello-Nachricht

- ProtocolVersion
- ServerRandom
- SessionID(nicht optional)
- Ciphersuites



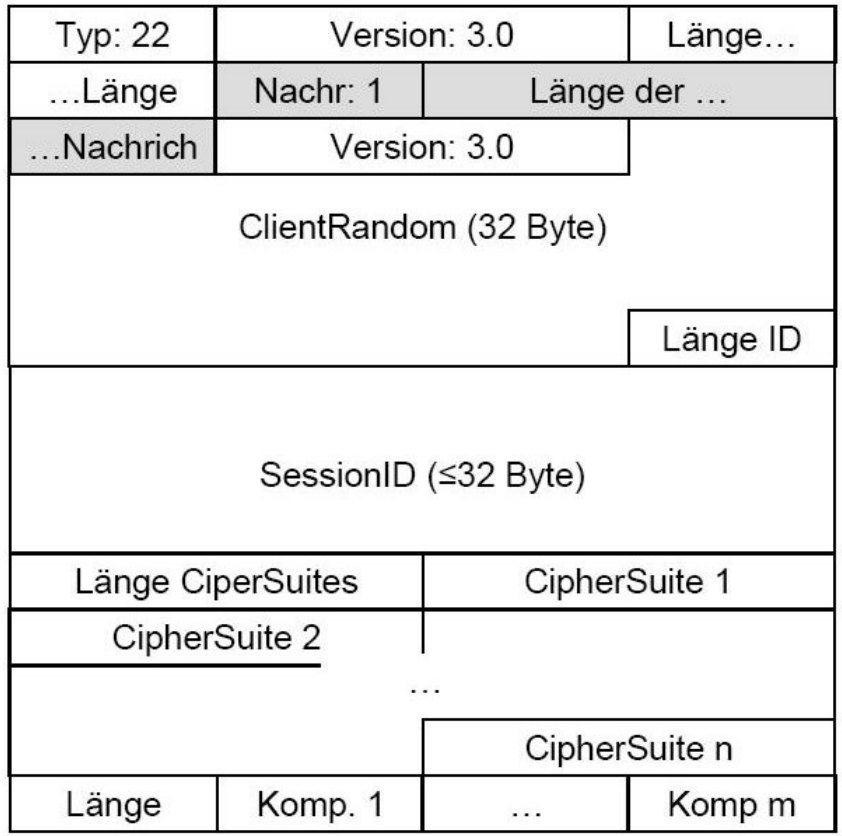
SSL Handshake-Nachrichten

ClientHello-Nachricht

- ProtocolVersion
- ClientRandom
- SessionID(optional)
- Ciphersuites

ServerHello-Nachricht

- ProtocolVersion
- ServerRandom
- SessionID(nicht optional)
- Ciphersuites



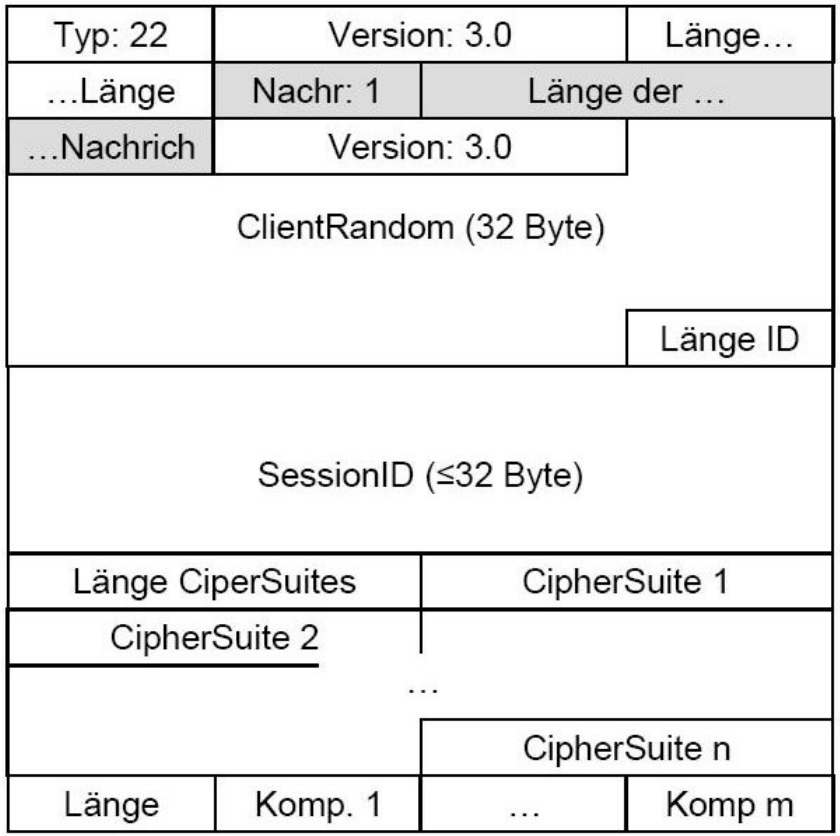
SSL Handshake-Nachrichten

ClientHello-Nachricht

- ProtocolVersion
- ClientRandom
- SessionID(optional)
- Ciphersuites

ServerHello-Nachricht

- ProtocolVersion
- ServerRandom
- SessionID(nicht optional)
- Ciphersuites



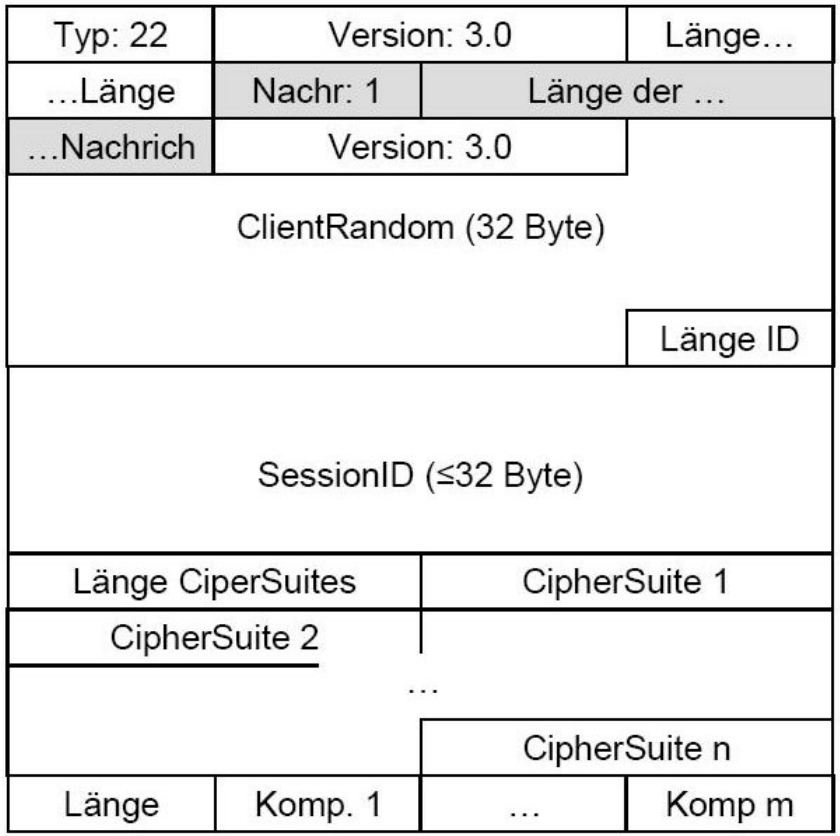
SSL Handshake-Nachrichten

ClientHello-Nachricht

- ProtocolVersion
- ClientRandom
- SessionID(optional)
- Ciphersuites

ServerHello-Nachricht

- ProtocolVersion
- ServerRandom
- SessionID(nicht optional)
- Ciphersuites



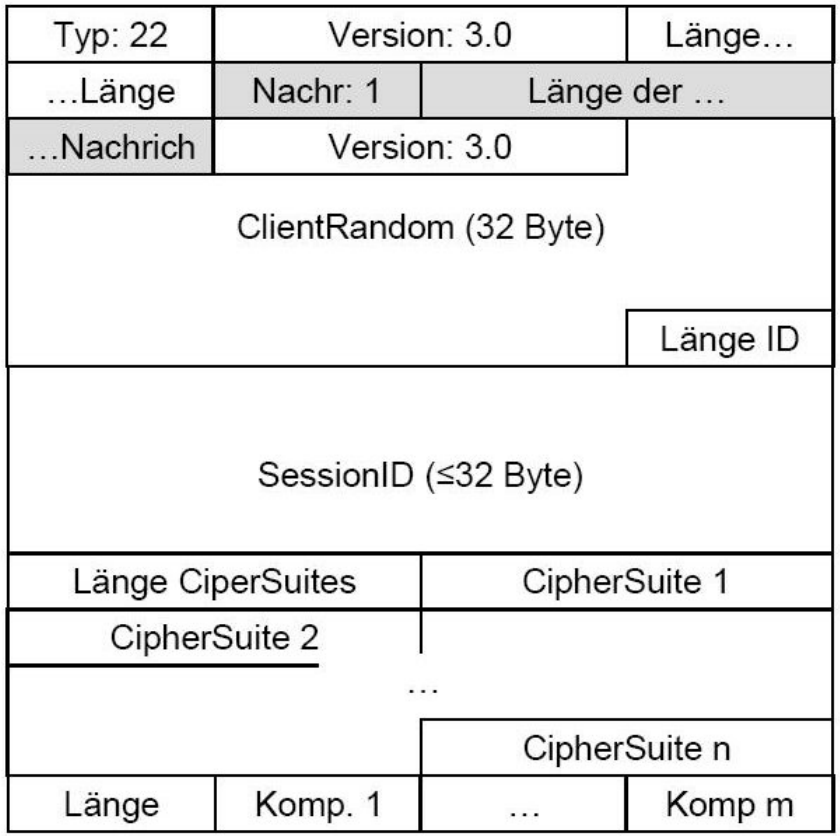
SSL Handshake-Nachrichten

ClientHello-Nachricht

- ProtocolVersion
- ClientRandom
- SessionID(optional)
- Ciphersuites

ServerHello-Nachricht

- ProtocolVersion
- ServerRandom
- SessionID(nicht optional)
- Ciphersuites



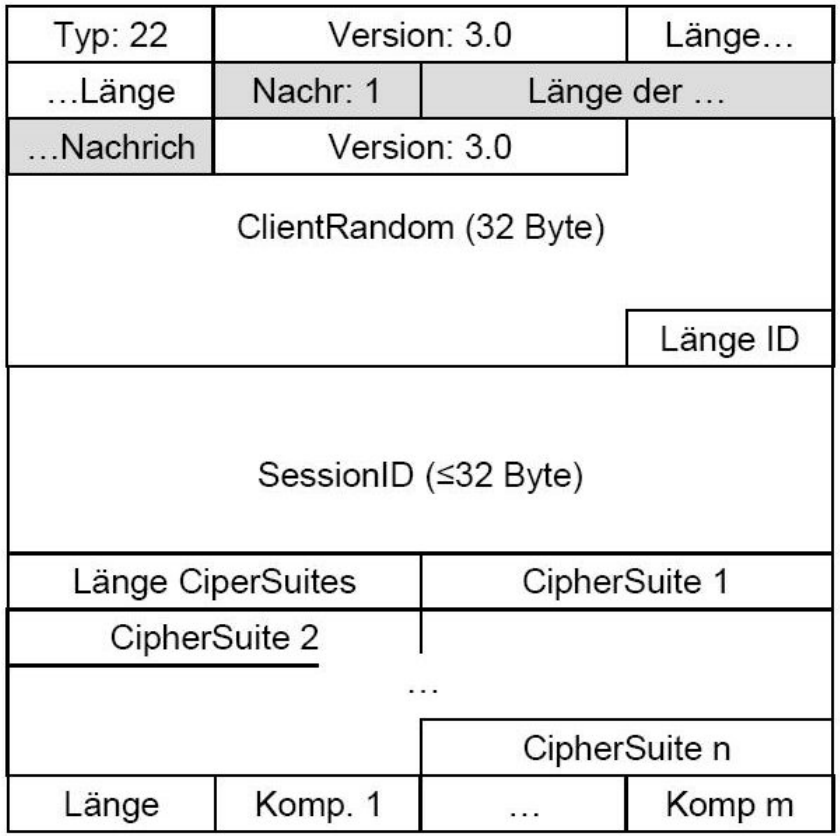
SSL Handshake-Nachrichten

ClientHello-Nachricht

- ProtocolVersion
- ClientRandom
- SessionID(optional)
- Ciphersuites

ServerHello-Nachricht

- ProtocolVersion
- ServerRandom
- SessionID(nicht optional)
- Ciphersuites



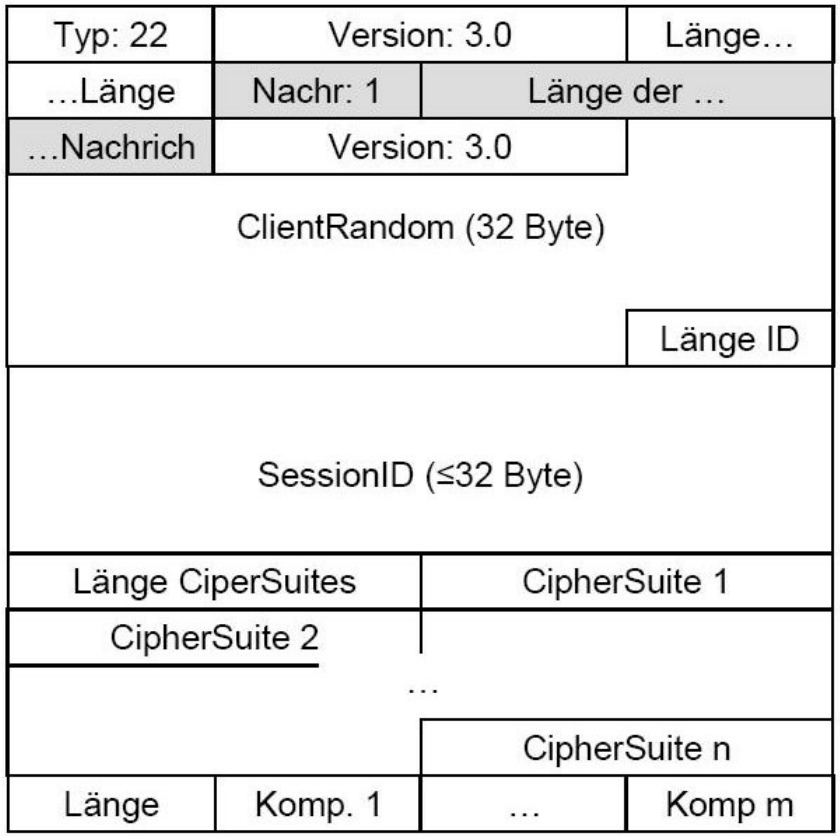
SSL Handshake-Nachrichten

ClientHello-Nachricht

- ProtocolVersion
- ClientRandom
- SessionID(optional)
- Ciphersuites

ServerHello-Nachricht

- ProtocolVersion
- ServerRandom
- SessionID(nicht optional)
- Ciphersuites



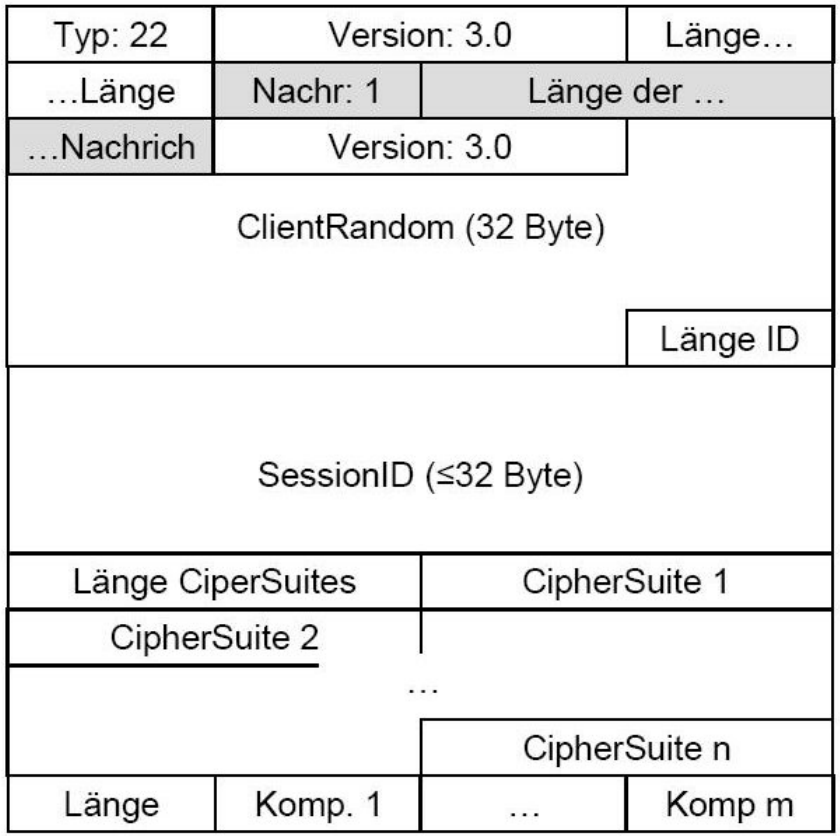
SSL Handshake-Nachrichten

ClientHello-Nachricht

- ProtocolVersion
- ClientRandom
- SessionID(optional)
- Ciphersuites

ServerHello-Nachricht

- ProtocolVersion
- ServerRandom
- SessionID(nicht optional)
- Ciphersuites



SSL Handshake-Nachrichten

ServerCertificate-Nachricht

- Server besitzt zertifizierten öffentlichen Schlüssel
- Inhalt: Server-Zertifikat X.509.v3

ServerKeyExchange-Nachricht

- Server besitzt kein Zertifikat oder nur zertifizierten Signaturschlüssel
- Inhalt: öffentlicher Schlüssel

ServerHelloDone-Nachricht

SSL Handshake-Nachrichten

ServerCertificate-Nachricht

- Server besitzt zertifizierten öffentlichen Schlüssel
- Inhalt: Server-Zertifikat X.509.v3

ServerKeyExchange-Nachricht

- Server besitzt kein Zertifikat oder nur zertifizierten Signaturschlüssel
- Inhalt: öffentlicher Schlüssel

ServerHelloDone-Nachricht

SSL Handshake-Nachrichten

ClientKeyExchange-Nachricht

- Inhalt: je nach möglicher Authentifikation
  - Keine Authentifikation
  - Server besitzt Zertifikat:pre master secret oder Zertifizierten Schlüssel für Diffie Hellmann Schlüsselvereinbarung
  - Client und Server besitzen Zertifikate für Diffie Hellmann

SSL Handshake-Nachrichten

ClientKeyExchange-Nachricht

- Inhalt: je nach möglicher Authentifikation
  - Keine Authentifikation
  - Server besitzt Zertifikat:pre master secret oder Zertifizierten Schlüssel für Diffie Hellmann Schlüsselvereinbarung
  - Client und Server besitzen Zertifikate für Diffie Hellmann

SSL Handshake-Nachrichten

ClientKeyExchange-Nachricht

- Inhalt: je nach möglicher Authentifikation
  - Keine Authentifikation
  - Server besitzt Zertifikat:pre master secret oder Zertifizierten Schlüssel für Diffie Hellmann Schlüsselvereinbarung
  - Client und Server besitzen Zertifikate für Diffie Hellmann

SSL Handshake-Nachrichten

ClientKeyExchange-Nachricht

- Inhalt: je nach möglicher Authentifikation
  - Keine Authentifikation
  - Server besitzt Zertifikat:pre master secret oder Zertifizierten Schlüssel für Diffie Hellmann Schlüsselvereinbarung
  - Client und Server besitzen Zertifikate für Diffie Hellmann

SSL Handshake-Change Cipher Spec-Protokoll und Finished-Nachricht

- Change Cipher Spec
  - Schlüssel für symmetrische Verschlüsselung und MAC-Algorithmus mittels Hash-Funktion über master secret berechenbar
  - Mitteilung der abgeschlossenen Berechnungen (Schlüssel aktiv)
- Finished
  - Master secret (Ergebnis des Handshakes)
  - Hashwert aller Handshake-Nachrichten

SSL Handshake-Change Cipher Spec-Protokoll und Finished-Nachricht

- Change Cipher Spec
  - Schlüssel für symmetrische Verschlüsselung und MAC-Algorithmus mittels Hash-Funktion über master secret berechenbar
  - Mitteilung der abgeschlossenen Berechnungen (Schlüssel aktiv)
- Finished
  - Master secret (Ergebnis des Handshakes)
  - Hashwert aller Handshake-Nachrichten

SSL Handshake-Change Cipher Spec-Protokoll und Finished-Nachricht

- Change Cipher Spec
  - Schlüssel für symmetrische Verschlüsselung und MAC-Algorithmus mittels Hash-Funktion über master secret berechenbar
  - Mitteilung der abgeschlossenen Berechnungen (Schlüssel aktiv)
- Finished
  - Master secret (Ergebnis des Handshakes)
  - Hashwert aller Handshake-Nachrichten

SSL Handshake-Change Cipher Spec-Protokoll und Finished-Nachricht

- Change Cipher Spec
  - Schlüssel für symmetrische Verschlüsselung und MAC-Algorithmus mittels Hash-Funktion über master secret berechenbar
  - Mitteilung der abgeschlossenen Berechnungen (Schlüssel aktiv)
- Finished
  - Master secret (Ergebnis des Handshakes)
  - Hashwert aller Handshake-Nachrichten

SSL Handshake-Change Cipher Spec-Protokoll und Finished-Nachricht

- Change Cipher Spec
  - Schlüssel für symmetrische Verschlüsselung und MAC-Algorithmus mittels Hash-Funktion über master secret berechenbar
  - Mitteilung der abgeschlossenen Berechnungen (Schlüssel aktiv)
- Finished
  - Master secret (Ergebnis des Handshakes)
  - Hashwert aller Handshake-Nachrichten

SSL Handshake-Change Cipher Spec-Protokoll und Finished-Nachricht

- Change Cipher Spec
  - Schlüssel für symmetrische Verschlüsselung und MAC-Algorithmus mittels Hash-Funktion über master secret berechenbar
  - Mitteilung der abgeschlossenen Berechnungen (Schlüssel aktiv)
- Finished
  - Master secret (Ergebnis des Handshakes)
  - Hashwert aller Handshake-Nachrichten

SSL Handshake-optionale Authentisierung des Clients

- implizite Authentisierung des Servers
- explizite Authentisierung des Clients (Certificate Request, Client Certificate, Certificate Verify)

SSL Handshake-optionale Authentisierung des Clients

- implizite Authentisierung des Servers
- explizite Authentisierung des Clients (Certificate Request, Client Certificate, Certificate Verify)

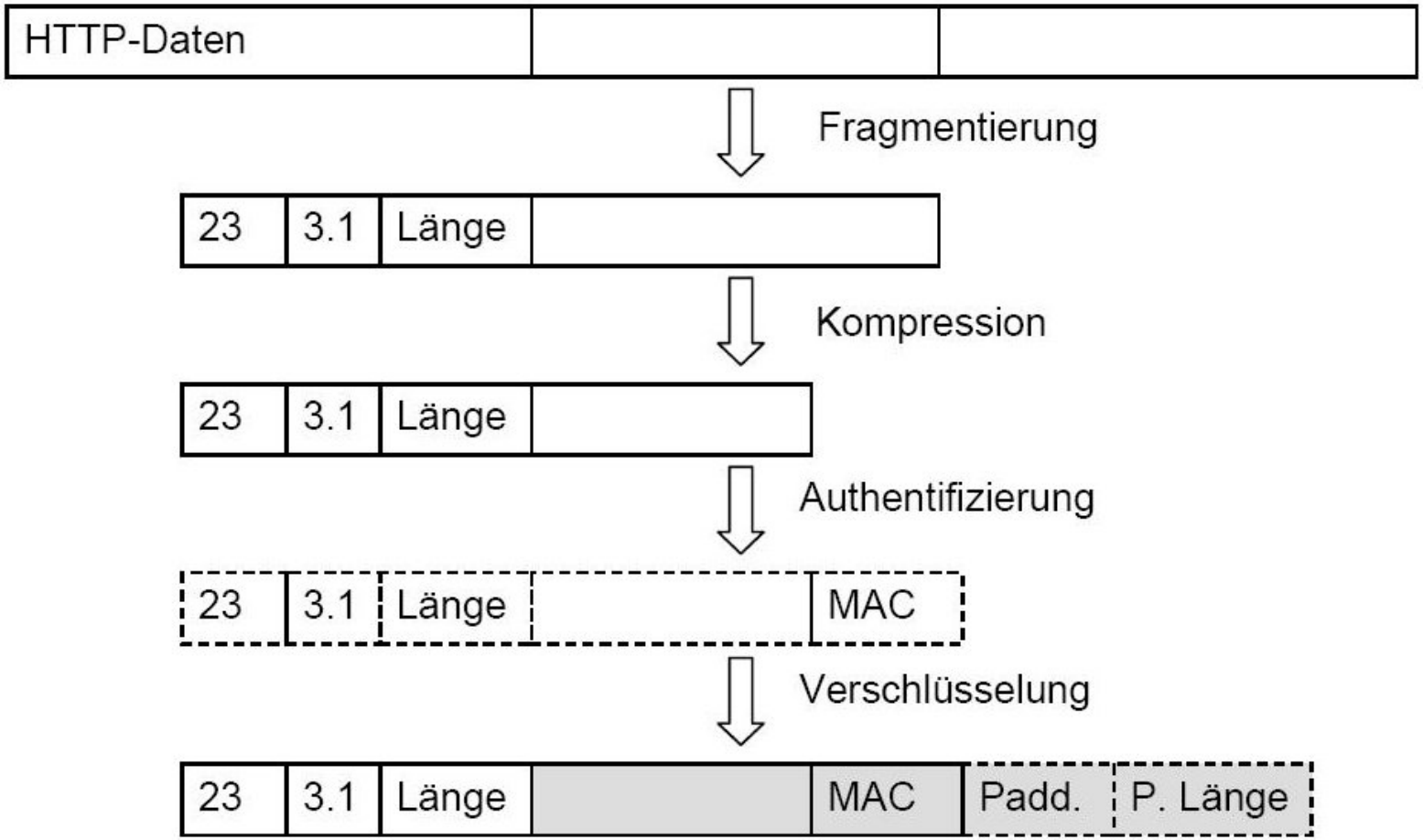
SSL-Alert Protokoll

- Fehlermeldung bzgl. der Art und Schwere des aufgetretenden Fehlers
- Zwei Fehlergrade: Warning und Fatal

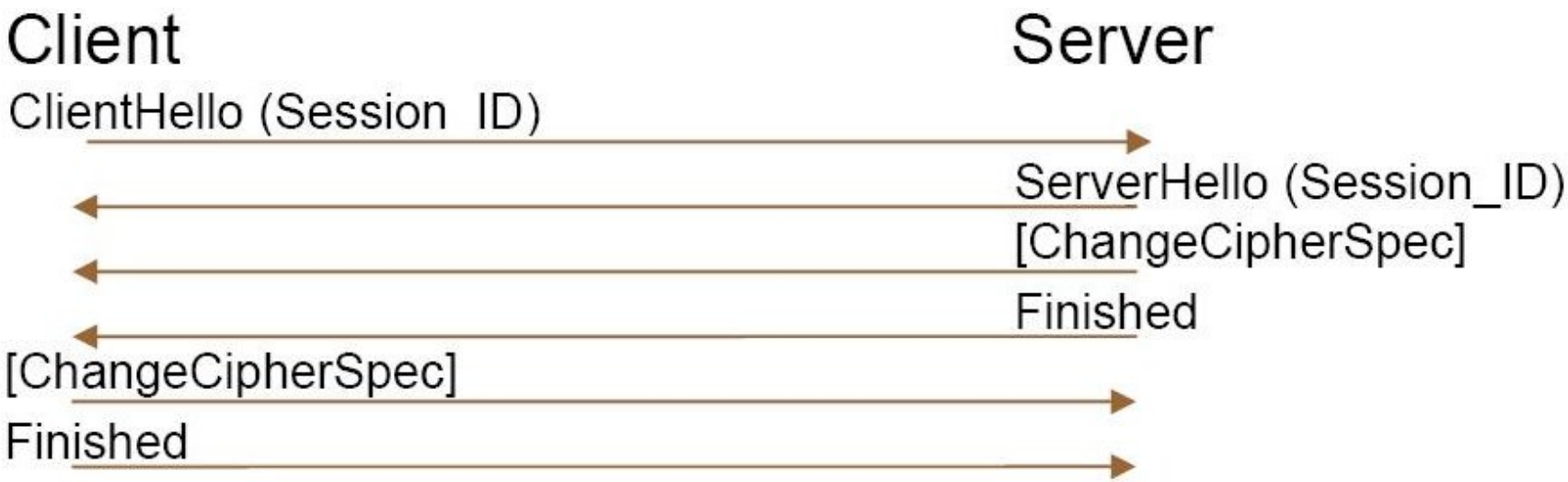
SSL-Alert Protokoll

- Fehlermeldung bzgl. der Art und Schwere des aufgetretenden Fehlers
- Zwei Fehlergrade: Warning und Fatal

SSL Record Layer Protokoll



SSL Handshake-Verkürzter SSL-Handshake



Transport Layer Security(TLS)

- SSL 3.1
- Internetstandard nach IETF
- Neue Alert-Nachrichten
- Änderungen betreffend:
  - Nachrichten-Authentifikation
  - Erzeugung des Schlüsselmaterials
  - Certificate Verify und Finished Nachricht
  - Herausnahme der Fortezza-Ciphersuites aus den zwingend vorgeschriebenen Suites

Transport Layer Security(TLS)

- SSL 3.1
- Internetstandard nach IETF
- Neue Alert-Nachrichten
- Änderungen betreffend:
  - Nachrichten-Authentifikation
  - Erzeugung des Schlüsselmaterials
  - Certificate Verify und Finished Nachricht
  - Herausnahme der Fortezza-Ciphersuites aus den zwingend vorgeschriebenen Suites

Transport Layer Security(TLS)

- SSL 3.1
- Internetstandard nach IETF
- Neue Alert-Nachrichten
- Änderungen betreffend:
  - Nachrichten-Authentifikation
  - Erzeugung des Schlüsselmaterials
  - Certificate Verify und Finished Nachricht
  - Herausnahme der Fortezza-Ciphersuites aus den zwingend vorgeschriebenen Suites

Transport Layer Security(TLS)

- SSL 3.1
- Internetstandard nach IETF
- Neue Alert-Nachrichten
- Änderungen betreffend:
  - Nachrichten-Authentifikation
  - Erzeugung des Schlüsselmaterials
  - Certificate Verify und Finished Nachricht
  - Herausnahme der Fortezza-Ciphersuites aus den zwingend vorgeschriebenen Suites

Transport Layer Security(TLS)

- SSL 3.1
- Internetstandard nach IETF
- Neue Alert-Nachrichten
- Änderungen betreffend:
  - Nachrichten-Authentifikation
  - Erzeugung des Schlüsselmaterials
  - Certificate Verify und Finished Nachricht
  - Herausnahme der Fortezza-Ciphersuites aus den zwingend vorgeschriebenen Suites

Transport Layer Security(TLS)

- SSL 3.1
- Internetstandard nach IETF
- Neue Alert-Nachrichten
- Änderungen betreffend:
  - Nachrichten-Authentifikation
  - Erzeugung des Schlüsselmaterials
  - Certificate Verify und Finished Nachricht
  - Herausnahme der Fortezza-Ciphersuites aus den zwingend vorgeschriebenen Suites

Transport Layer Security(TLS)

- SSL 3.1
- Internetstandard nach IETF
- Neue Alert-Nachrichten
- Änderungen betreffend:
  - Nachrichten-Authentifikation
  - Erzeugung des Schlüsselmaterials
  - Certificate Verify und Finished Nachricht
  - Herausnahme der Fortezza-Ciphersuites aus den zwingend vorgeschriebenen Suites

Transport Layer Security(TLS)

- SSL 3.1
- Internetstandard nach IETF
- Neue Alert-Nachrichten
- Änderungen betreffend:
  - Nachrichten-Authentifikation
  - Erzeugung des Schlüsselmaterials
  - Certificate Verify und Finished Nachricht
  - Herausnahme der Fortezza-Ciphersuites aus den zwingend vorgeschriebenen Suites

Analyse und Angriffe auf SSL

- Side Channel Attacks
  - "Million Question"Angriff
  - Framespoofing
  - Angriff auf ungeschütztes Versionsnummernfeld
  - Angriff auf ungeschütztes Schlüsselaustauschalgorithmusfeld
- Ansatz an Maschine-Schnittstelle
- SLS und TLS sicher

Analyse und Angriffe auf SSL

- Side Channel Attacks
  - “Million Question“Angriff
  - Framespoofing
  - Angriff auf ungeschütztes Versionsnummernfeld
  - Angriff auf ungeschütztes Schlüsselaustauschalgorithmusfeld
- Ansatz an Maschine-Schnittstelle
- SLS und TLS sicher

Analyse und Angriffe auf SSL

- Side Channel Attacks
  - “Million Question“Angriff
  - Framespoofing
  - Angriff auf ungeschütztes Versionsnummernfeld
  - Angriff auf ungeschütztes Schlüsselaustauschalgorithmusfeld
- Ansatz an Maschine-Schnittstelle
- SLS und TLS sicher

Analyse und Angriffe auf SSL

- Side Channel Attacks
  - “Million Question“Angriff
  - Framespoofing
  - Angriff auf ungeschütztes Versionsnummernfeld
  - Angriff auf ungeschütztes Schlüsselaustauschalgorithmusfeld
- Ansatz an Maschine-Schnittstelle
- SLS und TLS sicher

Analyse und Angriffe auf SSL

- Side Channel Attacks
  - “Million Question“Angriff
  - Framespoofing
  - Angriff auf ungeschütztes Versionsnummernfeld
  - Angriff auf ungeschütztes Schlüsselaustauschalgorithmusfeld
- Ansatz an Maschine-Schnittstelle
- SLS und TLS sicher

Analyse und Angriffe auf SSL

- Side Channel Attacks
  - “Million Question“Angriff
  - Framespoofing
  - Angriff auf ungeschütztes Versionsnummernfeld
  - Angriff auf ungeschütztes Schlüsselaustauschalgorithmusfeld
- Ansatz an Maschine-Schnittstelle
- SLS und TLS sicher

Analyse und Angriffe auf SSL

- Side Channel Attacks
  - “Million Question“Angriff
  - Framespoofing
  - Angriff auf ungeschütztes Versionsnummernfeld
  - Angriff auf ungeschütztes Schlüsselaustauschalgorithmusfeld
- Ansatz an Maschine-Schnittstelle
- SLS und TLS sicher