Konzepte von Betriebssystem-Komponenten
Schwerpunkt Internetsicherheit

Secure Socket Layer V.3.0

(SSLv3)

Zheng Yao

05.07.2004

Überblick

1.Was ist SSL?

Bestandteile von SSL-Protokoll, Verbindungherstellung mit SSL hello, SSL Versionen

2. Digitale Authentifizierung

Public Key Zertifikate, Die von SSL unterstützten Zertifikate, Authentifizierung von Server und Client

3. SSL/TLS Features

Verschiedene Algorithmen, Effizienz, Authentifizierung, Unterstützen für Kompression
Schutz vor man-in-middle- und replay- Angriffe, Kompatibilität mit SSLv2
.....

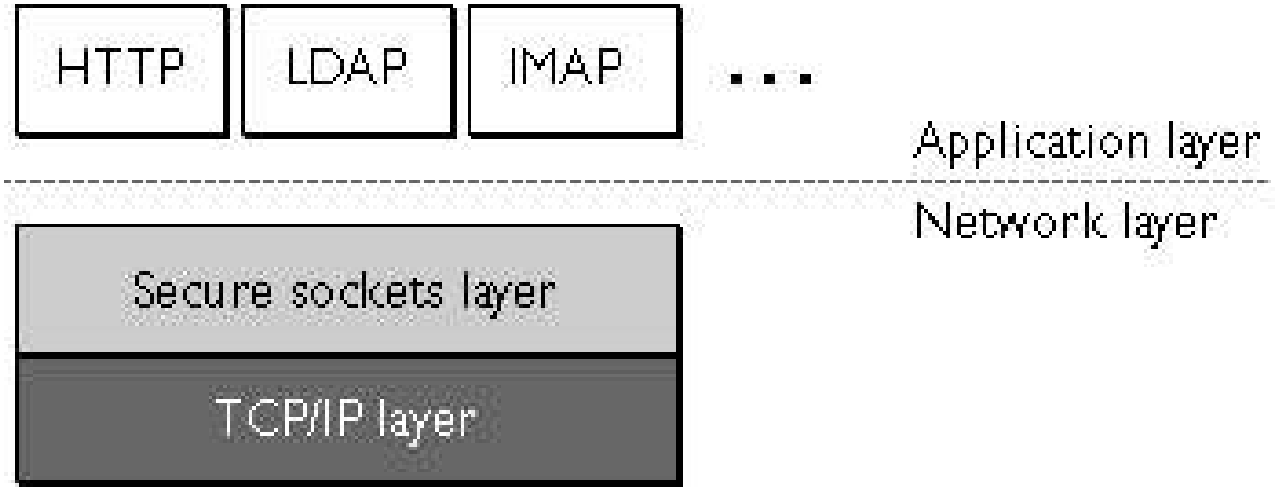
4. SSL Implementierungen

SSL Netscape, SSLRef und Mozilla NSS, SSLeay und OpenSSL, SSL Java

Was ist SSL?

Secure Soket Layer, Protokoll zur Übertragung von verschlüsselten Informationen.

- 1994 von Netscape entwickelt.
- Es befinedt sich zwischen Anwendungsschicht und Transportschicht
- Es läuft auf TCP/IP , wird von HTTP,LDAP,IMAP etc. benutzt.



SSL Protokoll

SSL wurde für den Einsatz zwischen Client und Server entwickelt und besteht wesentlich aus drei Teilen:

Das Record-Protokoll

- wie eine zusätzliche Schicht über allen SSL- Nachrichten
- die angewandeten Verschlüsselungs- und Authentifizierungsfunktionen angeben

Das Handshake-Protokoll

- Damit können Client und Server den Einsatz von kryptographischen Algorithmen und Schlüsseln behandeln
- Damit wird die SSL-Verbindung aufgebaut

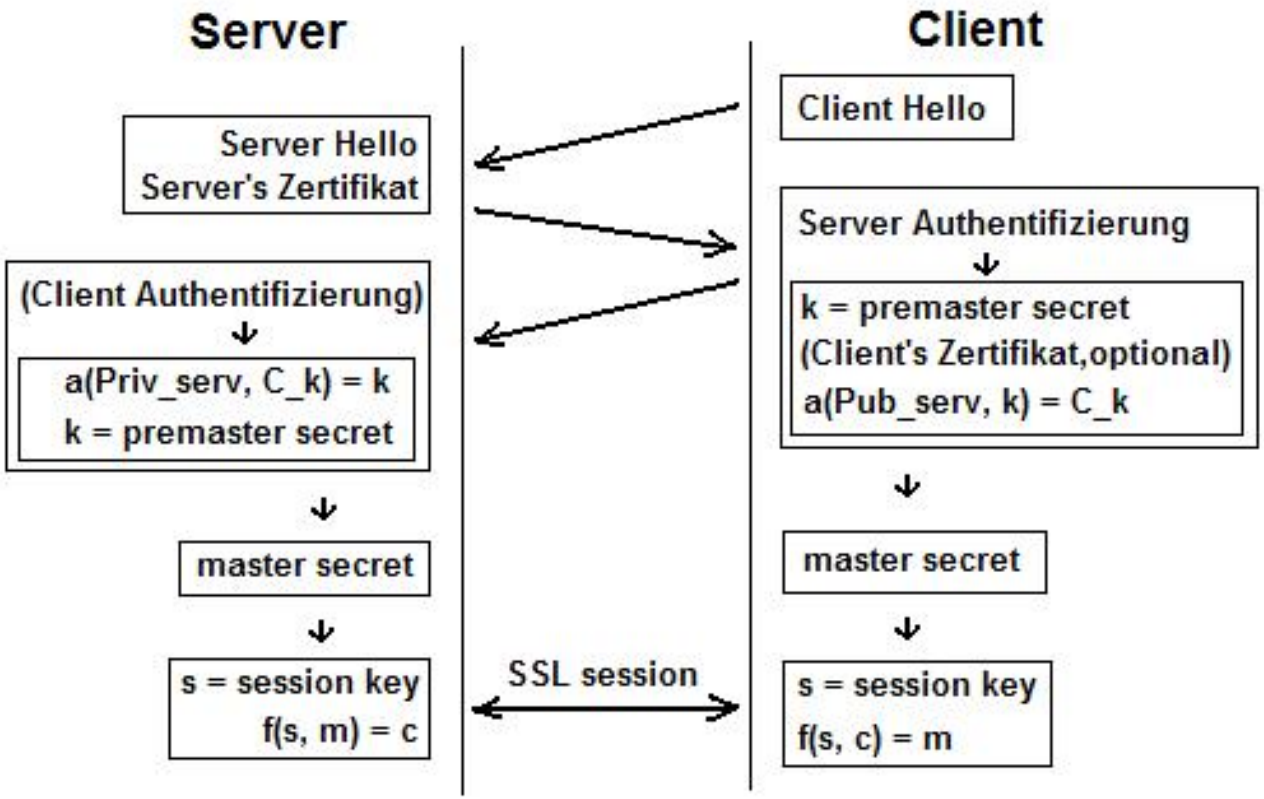
Das Alert-Protokoll

Signale an Server oder Client senden , wenn:

- Auftreten von Fehlern
- Abbruch einer Kommunikationsverbindung

SSL Hello

Wie wird eine Kommunikationsverbindung mit SSL hergestellt?



SSL Versionen

SSL Version 1 und 2

- verwendet in Server und Navigator von Netscape
- Microsoft hat eine SSLv2 Inplementierung, PCT
- SSLv2 wird jetzt noch für längere Zeit beibehalten

SSL Version 3

- neueste Version

TLS (Transport Layer Security)

- eigentlich Version 3.1 von SSL
- auf SSLv3 basieren
- ein neues standardisiertes Sicherheitsprotokoll
- entwickelt von IETF(Internet Engineering Task Force)

Digitale Authentifizierung

SSL benutzt **Public Key Zertifikate** für die Authentifizierung von Server und Client.

SSL unterstützt die folgende Zertifikate:

- RSA public key Zertifikate, deren Keys können beliebige Länge haben.

  RSA, (Drei Erfinder, Rivest, Shamir, und Adelman)

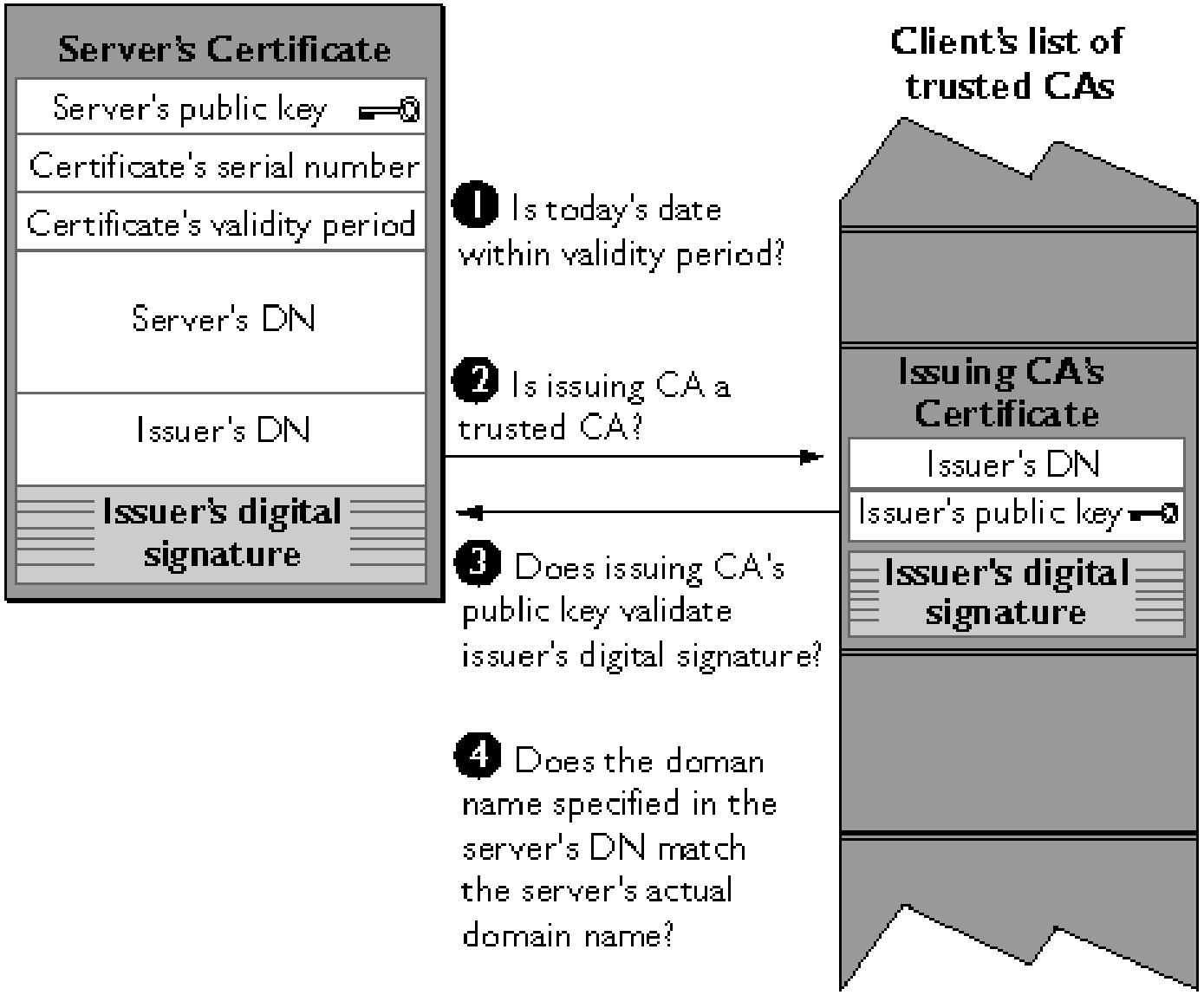
- RSA public key Zertifikate, deren keys sind nur 512 bits.
  Für besondere Anwendung mit Beschränkung von Kryptographie.

- Signing-only RSA Zertifikate, die nur für Signieren der Daten sind.
  Nicht für Verschlüsselung von Daten.

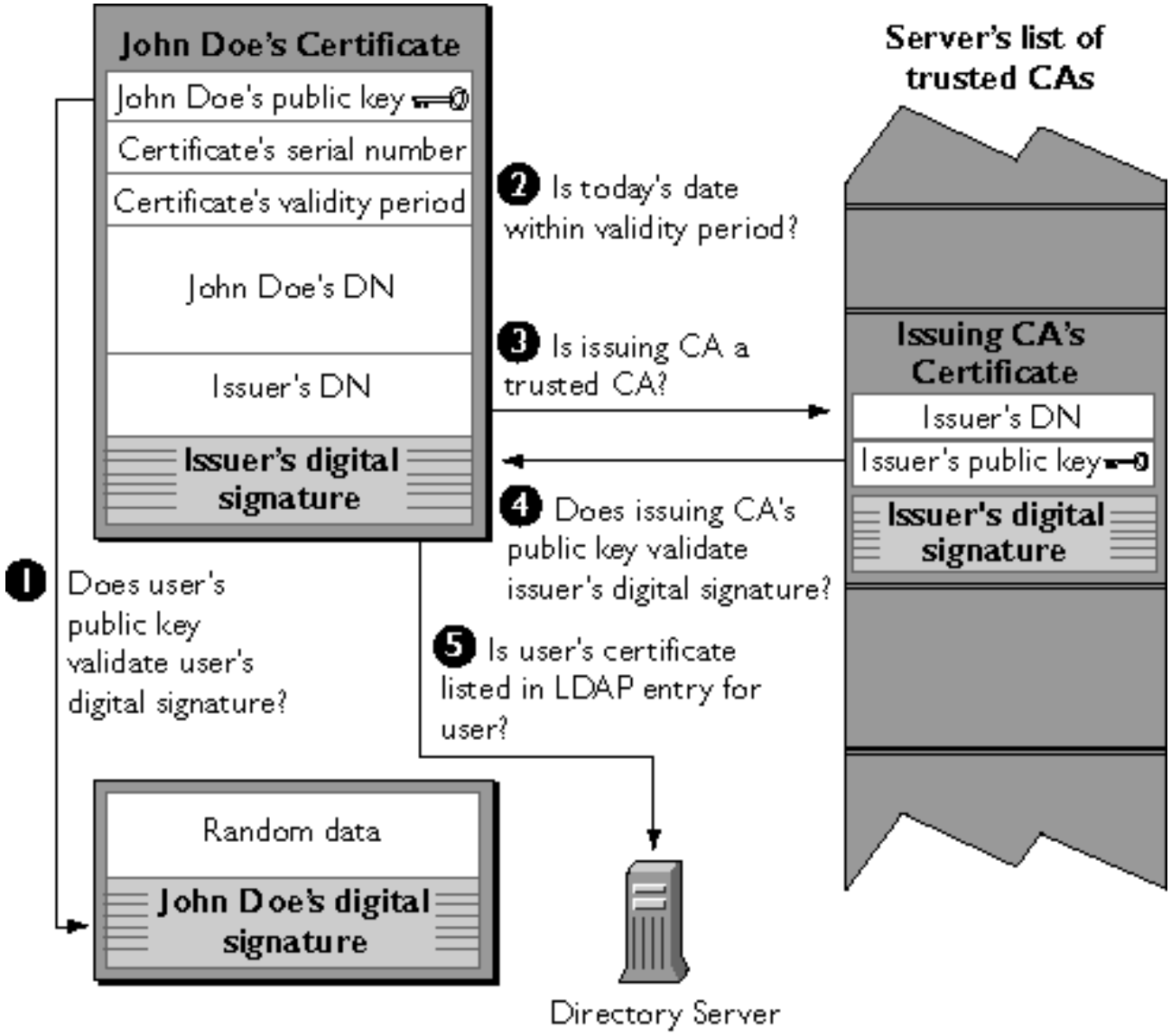
- DSS Zertifikate *(the Digital Signature Standard)*

- Diffie-Hellman Zertifikate

Server Authentifizierung



Client Authentifizierung (optional)



SSL Features

Verschiedene Algorithmen für die Aufgaben

- Verschiedene Algorithmen für Verschlüsselung, Authentifizierung und Vollständigkeit der Daten
- Verschiedene Länge von Schlüsseln
- erlaubt die nicht verschlüsselte aber authentifizierte Verbindung

Effizienz

- Problem: viel Zeit für Verschlüsselung und Entschlüsselung der Public Keys
- „master secret“ generieren
- weitere Kommunikationen mit symmetrischen Verfahren sicher durchgeführt werden

SSL Features

Auf Zertifikate basierende Authentifizierung

- SSL bietet die Authentifizierung von Server und auch von Client an
- SSLv3 und TLS benutzen X.509 Zertifikate

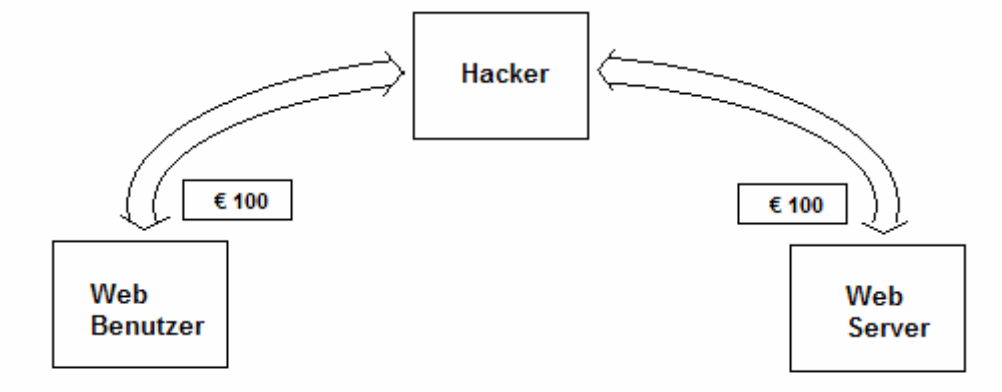
  X.509, ein Standard von Zertifikat, die Struktur von Zertifikat definieren
- Die Authentifizierung von Client ist optional

Protokoll agnostisch

- nicht nur auf TCP/IP, sondern auch auf viele andere zuverlässige Protokolle in der Transportschicht, z.B.: X.25.
- nicht über die unzuverlässigen Protokollen wie IP User Datagram Protocoll(UDP).

SSL Features

Schutz vor man-in-the-middle- und replay- Angriff

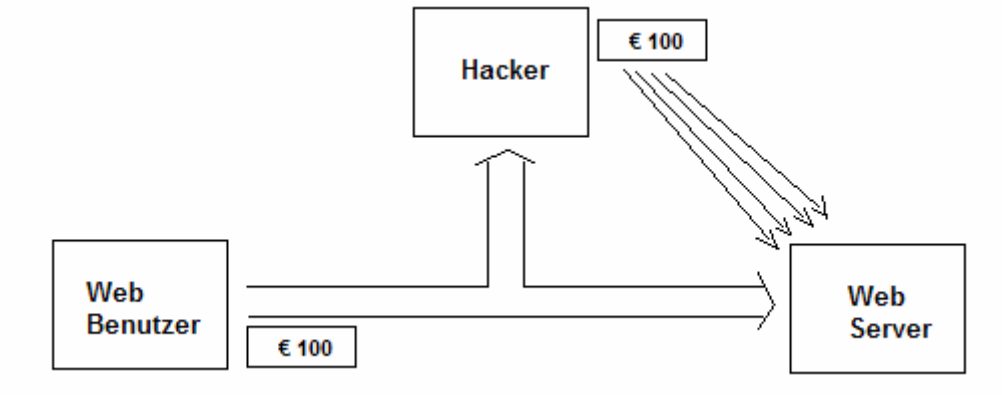


man-in-the-middle-Angriff

- Alle Informationen zwischen Server und Client werden von Hacker gefangen
- Server und Benutzer denken immer, dass sie nur miteinander kommunizieren.

SSL Features

Schutz vor man-in-the-middle- und replay- Angriff



replay- Angriff

- der Hacker fängt die Informationen von Zahlungsnachrichten
- Durch die Wiederholung dieser Nachrichten schafft der Hacker die illegalen Transaktionen.

SSL benutzt digitalle Authentifizierung gegen diese Angriffe

SSL Features

Unterstützung von Kompression

- Problem: die gut verschlüsselten Daten können nicht mehr komprimiert werden.
- die Daten komprimieren vor der Verschlüsselung.

Ruckwärts Kompatibilität mit SSL V.2.0

- SSLv3 Server kann auch die Verbindung von SSLv2 Client aufnehmen
- Sie behandeln sofort die SSL-Nachrichten, ohne eine neue Verbindung dazwischen aufzubauen.

SSL Implementierungen

SSL Netscape

- erste SSL Implementierung
- nur in Netscape´s Webbrowser und Webserver implementiert

SSLRef und Mozilla Network Security Services(NSS)

SSLRef

- eine Referenz-implementierung von SSL
- Nicht mehr verfügbar und ersetzt von Mozilla NSS.

Mozilla Network Security Services(NSS)

- eine große Menge von Bibliotheken für die Entwicklung für Internetsicherheit.
- NSS unterstützt SSLv2, SSLv3, TLS und viele andere Internetsicherheitsstandards
- Projekt Home: http://www.mozilla.org/projects/security/pki/nss/

SSL Implementierungen

SSLeay und OpenSSL

SSLeay

- eine selbständige Implementierung von SSL v.3.0
- von zwei australische Programmer Eric A.Young und Tim Hudson entwickelt

OpenSSL

- basiert auf SSLeay.
- Die wichtigste Entwickelungsprojekt von SSL
- die Basis von SSL Implementierung in Apache Web Server.
- Projekt Home: http://www.openssl.org

SSL Java

- Sun´s Java bietet die Cryptography Extensions für Internetsicherheit
- JSAFE von RSA Data Security

Zusamenfassung

1.Was ist SSL?

Bestandteile von SSL-Protokoll, Verbindungherstellung mit SSL hello, SSL Versionen

2. Digitale Authentifizierung

Public Key Zertifikate, Die von SSL unterstützten Zertifikate, Authentifizierung von Server und Client

3. SSL/TLS Features

Verschiedene Algorithmen, Effizienz, Authentifizierung, Unterstützen für Kompression
Schutz vor man-in-middle- und replay- Angriffe, Kompatibilität mit SSLv2
.....

4. SSL Implementierungen

SSL Netscape, SSLRef und Mozilla NSS, SSLeay und OpenSSL, SSL Java

Quellen

[1] Richard E.Smith Boon, Internet-Kryptographie, Addison-Wesley-Longman, 1998

[2] Simson Garfinkel with Gene Spafford, Web Security, Privacy, and Commerce (2nd Edition), O'Reilly, 2002

[3] Alan O. Freier, Philip Karlton, Paul C. Kocher, Netscape, The SSL Protocol Version 3.0, http://wp.netscape.com/eng/ssl3/ssl-toc.html, stand: March 1996

[4] Netscape, Introduction to SSL, http://developer.netscape.com/docs/manuals/security/sslin/, stand: Sept. 1998

[5] T. Dierks, C. Allen, The TLS 1.0 Protocol, http://www.ietf.org/rfc/rfc2246.txt, stand: January 1999

[6] The OpenSSL Project, http://www.openssl.org, stand: Juni 2004

[7] The Network Security Services Project (NSS), http://www.mozilla.org/projects/security/pki/nss/, stand: Juni 2004.