DuD
Datenschutz und Datensicherheit

Das Royal Holoway-System

Ein Key Recovery-Protokoll für Europa?

Dirk Fox

Im Herbst 1995 wurde von britischen Kryptologen ein Key Recovery-Protokoll publiziert, das eine Reihe von Eigenschaften besitzt, die es auf den ersten Blick für einen internationalen Einsatz geeignet erscheinen lassen. Das Protokoll wird derzeit von der britischen CESG (Communications-Electronics Security Group) für die verschlüsselte Kommunikation der Regierungsbehörden protegiert.

Der Beitrag skizziert die Funktionsweise dieses Protokolls, das in der EU schon als möglicher Key Recovery-Standard für Europa diskutiert wurde, und faßt die wichtigsten (technischen) Kritikpunkte zusammen.

Dipl.-Inform.
Dirk Fox

Security Consultant,
r³ security engineering ag, Karlsruhe.

Arbeitsgebiete: Digitale Signatursysteme, Trust Center, Sicherheit von Rechnernetzen.
E-Mail: fox@r3sec.de

1 Einleitung

Seit der Normung eines Key Escrow-Systems in den USA, dem *Escrowed Encryption Standard* (EES) [NIST_94, Ruep_94], sind eine Vielzahl von Schlüsselhinterlegungssystemen konzipiert und vorgeschlagen worden.

Die dabei gewonnenen Erfahrungen und die öffentliche Diskussion des EES haben zu einer Verfeinerung der Konzepte geführt: Statt einer Hinterlegung von Master-Schlüsseln werden nun Systeme propagiert, die eine Rückgewinnung temporärer Kommunikationsschlüssel (*Key Recovery*[1]) bzw. eine Rückgewinnung der Klartext-Daten oder -Nachrichten (*Data* resp. *Message Recovery*) erlauben.[2]

Da eine rechtliche Vereinheitlichung von Abhörgesetzen und der Regulierung von Kryptographie wegen der stark unterschiedlichen nationalen Gesetzgebung in der Europäischen Union in absehbarer Zeit nicht zu erwarten ist, suchen die europäischen Sicherheitsbehörden seit einer Weile nach technischen Lösungen, die ein europaweit einheitliches Key Recovery-Verfahren für die grenzüberschreitende Kommunikation bei gleichzeitiger Erhaltung der nationalen „Schlüsselsouveränität“ ermöglichen. Verschlüsselte innerstaatliche Kommunikation soll dabei fremden Sicherheitsbehörden bei einer Abhörmaßnahme nicht zugänglich werden.

Ein solches Key Recovery-Protokoll, das „*Royal Holloway Scheme*“, wurde 1995 am Royal Holloway College in London entwickelt. Es hat in Großbritannien Eingang in die Spezifikation einer Schlüssel-Infrastruktur für vertrauliche Behörden-Kommunikation gefunden und wurde von der britischen Regierung als europäischer Standard vorgeschlagen. Auch von einigen anderen europäischen Sicherheitsbehörden wird dieses Protokoll unterstützt (siehe z.B. für das BSI [Heus_95]).

[1] Siehe auch Fox, Gateway, DuD 4/1997, S. 227.

[2] Siehe auch Gerling, Company Message Recovery, Gateway, in diesem Heft.

2 Das Royal Holloway-System

Im Rahmen eines britischen Forschungsprojekts, den „Third Generation Systems Security Studies“ unter Beteiligung von Vodafone Ltd., GPT Ltd. und der Information Security Group des Royal Holloway College (University of London) wurde ein Key Recovery-Protokoll entwickelt, das 1995 als „Architecture for Trusted Third Party Services“ vorgestellt wurde [JeMW_95]. Eine überarbeitete Version, die Maßnahmen gegen einige Schwächen des ersten Entwurfs umfaßte, erschien 1996 [JeMW_96].

Das Protokoll wurde inzwischen von der britischen *Communications-Electronics Security Group* (CESG) der *Gouvernment Communication Headquaters* (GCHQ) in die Spezifikation einer Infrastruktur für vertrauliche elektronische Kommunikation der Regierungsbehörden (*Her Majesty's Government*, HMG) übernommen, zunächst für E-Mail (21. März 1996, [CESG_96]), später für jede Form der vertraulichen Behörden-Kommunikation (4. Februar 1997, [CESG_97]).

Anders als im amerikanischen EES wird in dem vorgeschlagenen Protokoll (im folgenden kurz „*GCHQ-Protokoll*“ genannt) der Zugriff der Sicherheitsbehörden auf verschlüsselte Nachrichten nicht durch das Mitsenden des verschlüsselten Session Keys in einem *Law Enforcement Access Field* (LEAF) ermöglicht: Gelang es dort einem Angreifer oder den Sicherheitsbehörden, Kenntnis von dem hinterlegten *Unit Key* (KU) zu erlangen, konnte jede zukünftige und zurückliegende verschlüsselte Kommunikation des sendenden Teilnehmers entschlüsselt werden. Ein Schlüsselwechsel

erforderte den Austausch des Clipper-Chips (siehe z.B. [Fox_95]).

Das GCHQ-Protokoll ist im Kern ein asymmetrisches, auf dem *Diffie-Hellman-Verfahren* (DH, siehe Anhang) beruhendes Schlüsselvereinbarungsprotokoll, bei dem die geheimen Verschlüsselungs-Schlüssel zweier Kommunikationsteilnehmer von (nationalen) Trusted Third Parties (TTPs), auch Certificate Management Authority (CMA) genannt [CESG_96], erzeugt, an die Teilnehmer übersendet und hinterlegt werden.

Das Protokoll hat die spezielle Eigenschaft, daß bei Vorliegen einer Abhöranordnung keine geheimen Schlüssel preisgegeben werden müssen, die ein Entschlüsseln einer anderen als der Kommunikationsbeziehung ermöglichen, für die die gerichtliche Anordnung vorliegt. Insbesondere ist für das Abhören verschlüsselter zwischenstaatlicher Kommunikation kein Zugriff auf ausländische Trusted Third Parties erforderlich. Schließlich können Teilnehmer jederzeit eine Neugenerierung ihrer geheimen Schlüssel verlangen.

3 Das GCHQ-Protokoll

Für die Vereinbarung eines gemeinsamen Schlüssels über Landesgrenzen hinweg sieht das GCHQ-Protokoll die Einrichtung nationaler Trusted Third Partys vor. Jede dieser TTPs ist für die Erzeugung der Kommunikationsschlüssel der Teilnehmer ihres Bereichs mit Teilnehmern anderer (z.B. ausländischer) TTPs zuständig. Damit bei Vorliegen einer Abhöranordnung nur ein Zugriff auf die geheimen Schlüssel der jeweils zuständigen TTP erforderlich ist, werden getrennte (asymmetrische) Sende- und Empfangsschlüsselpaare verwendet.

Die geheimen Schlüssel werden von der jeweils zuständigen TTP für den Teilnehmer erzeugt und diesem geheim übermittelt. Das gesamte Protokoll setzt sich aus vier Phasen zusammen:

3.1 Initialisierungsphase

Alle TTPs einigen sich paarweise auf gemeinsame DH-Parameter g und p (dabei ist p eine große, mindestens 768 bit lange Primzahl und g ein Generator des endlichen Körpers GF(p)). Um sicher vor bestimmten Maskerade-Angriffen zu sein, sollten jeweils unterschiedliche Paare (p, q) gewählt werden.

Für die Schlüsselgenerierung vereinbaren nun alle TTPs paarweise einen gemeinsamen geheimen (symmetrischen) Schlüssel k (z.B. mit einer Variante des DH-Protokolls wie dem von Diffie, Oorschot und Wiener vorgeschlagenen *Station-to-Station*-Protokoll [DiOW_92]).

Schließlich wählt jede TTP ein eigenes Signaturschlüsselpaar und veröffentlicht den Prüfschlüssel auf authentische Weise (z.B. durch Nutzung eines Zertifizierungs- und Verzeichnisdienstes einer vertrauenswürdigen Schlüssel-Infrastruktur).

3.2 Schlüsselgenerierung

Für jeden Teilnehmer erzeugt die zuständige TTP ein asymmetrisches Sendeschlüssel-Paar nach folgendem Verfahren: Sie wählt zunächst einen geheimen Master-Sendeschlüssel x_s zufällig[3] und übersendet diesen geschützt an den Teilnehmer. Aus diesem Master-Schlüssel und einem „Datumsstempel“ D leiten nun Teilnehmer und TTP mit einer festgelegten kryptographischen Einwegfunktion f (z.B. einer Hashfunktion) einen geheimen Tages-Sendeschlüssel $x_{s,D}$ ab:

$$x_{s,D} = f(x_s, D)$$

und bestimmen einen zugehörigen öffentlichen Tages-Sendeschlüssel $y_{s,D}$ mit

$$y_{s,D} = g^{x_{s,D}} \bmod p$$

Zu diesem öffentlichen Schlüssel stellt die TTP ein für den Tag D gültiges Zertifikat $Cert(y_{s,D}, D)$ aus, das sie dem Teilnehmer zugänglich macht (z.B. durch Veröffentlichung in einem Schlüsselverzeichnis).

Auf Wunsch des Teilnehmers ist der Master-Sendeschlüssel zu wechseln (d.h. neu zu wählen).

Zusätzlich wird für jeden gewünschten Empfänger einer Nachricht, der dem Zuständigkeitsbereich einer anderen TTP angehört, ein geheimer Master-Sendeschlüssel x_r bestimmt. Dieser wird nicht zufällig gewählt, sondern mit einer kryptographischen Einwegfunktion h (z.B. einer Hashfunktion) aus der Identität des Empfängers I_U und dem zwischen den zuständigen TTPs vereinbarten geheimen Schlüssel k sowie der Nummer I_K des neuen Master-Sendeschlüssels abgeleitet:[4]

$$x_r = h(k, I_U, I_K)$$

Analog der Bestimmung des Sendeschlüssels wird aus x_r ein geheimer Tages-Empfangsschlüssel abgeleitet:

$$x_{r,D} = f(x_r, D)$$

Den zugehörigen öffentlichen Tages-Empfangsschlüssel $y_{r,D}$ bestimmt die TTP durch eine Potenzierung:

$$y_{r,D} = g^{x_{r,D}} \bmod p$$

Die TTP zertifiziert diesen Schlüssel ebenfalls und veröffentlicht das Zertifikat $Cert(y_{r,D}, D)$ in einem Schlüsselverzeichnis oder leitet es auf Anfrage direkt an den Teilnehmer weiter.

3.3 Verschlüsselung

Will nun Teilnehmerin Alice (A) an Bob (B), der einer anderen TTP zugehört, eine vertrauliche Nachricht m senden, dann besorgt sie sich das Tages-Empfangsschlüssel-Zertifikat von Bob aus dem Schlüsselverzeichnis ihrer TTP bzw. fordert es bei ihrer TTP an.

Aus ihrem geheimen Tages-Sendeschlüssel $x_{A,D}$ für die Kommunikation mit Teilnehmern der TTP von Bob und Bobs öffentlichen Empfangsschlüssel $y_{B,D}$ bestimmt sie einen gemeinsamen geheimen DH-Schlüssel k_{AB}:

$$k_{AB} = y_{B,D}^{\,x_{A,D}} \bmod p$$

Anschließend wählt sie einen zufälligen *Session Key* ks, den sie mit einem Verschlüsselungsalgorithmus E und dem gemeinsamen Schlüssel k_{AB} verschlüsselt:

$$T_{ks} = E(k_{AB}, ks)$$

Diesen Schlüssel-Token sendet sie zusammen mit dem Zertifikat ihres öffentlichen Sendeschlüssels $y_{A,D}$, dem Zertifikat des verwendeten öffentlichen Empfangsschlüssels $y_{B,D}$ von Bob und der mit ks verschlüsselten Nachricht m

$$c = E(ks, m)$$

an Bob.

Bob berechnet aus dem öffentlichen Sendeschlüssel $y_{A,D}$ von Alice (dessen Authentizität und Integrität durch das mitgesendete Zertifikat bestätigt wird) und seinem geheimen Empfangsschlüssel $x_{B,D}$ für die Kommunikation mit Teilnehmern der TTP von Alice (den er ggf. von seiner TTP

[3] Es wurde auch vorgeschlagen, diesen geheimen Master-Sendeschlüssel ebenso wie den geheimen Master-Empfangsschlüssel zu erzeugen [CESG_97]. Das schafft jedoch einen überflüssigen zusätzlichen Angriffspunkt.

[4] Als kryptographische Einwegfunktionen f und g können unterschiedliche Funktionen gewählt werden.

anfordern muß) den gemeinsamen geheimen DH-Schlüssel k_{AB}:

$$k_{AB} = y_{A,D}^{x_{B,D}} \bmod p$$

Mit diesem entschlüsselt er den Token T_{ks} und erhält den von Alice zur Verschlüsselung der Nachricht verwendeten Session Key *ks*, mit dem er schließlich die Nachricht *c* entschlüsseln kann.

Vorteil der deterministischen Bestimmung des geheimen Empfangsschlüssels in diesem Protokoll ist, daß der öffentliche Tages-Empfangsschlüssel eines Teilnehmers aus einer fremden Domäne von jeder TTP bestimmt werden kann, ohne daß eine Nachfrage bei der zuständigen TTP erforderlich wäre. Dies verringert erstens den (grenzüberschreitenden) Kommunikationsaufwand und erlaubt zweitens den nationalen Sicherheitsbehörden, den Session Key ohne Zugriff auf ausländische TTPs wiederzugewinnen.

3.4 Key Recovery

Bei Vorliegen einer Abhöranordnung erhalten nun nationale Sicherheitsbehörden von der zuständigen TTP die geheimen Tages-Empfangsschlüssel für den Gültigkeitszeitraum der Anordnung. Wie der eigentliche Empfänger der Nachricht entnehmen sie der abgehörten Kommunikation den vom Sender verwendeten öffentlichen Tages-Sendeschlüssel und können daraus den verwendeten geheimen DH-Schlüssel k_{AB} bestimmen. Mit diesem entschlüsseln sie den Token T_{ks} und erhalten damit den verwendeten Session Key *ks*.

4 Bewertung

Das Verfahren wurde von den Kryptologen Ross Anderson und Michael Roe auf der diesjährigen internationalen Krypto-Konferenz Eurocrypt '97[5] einer intensiven Kritik unterzogen [AnRo_96, AnRo_97]. Im folgenden weden die wesentlichen Kritikpunkte zusammengefaßt.

4.1 Komplexität

In dem vorgeschlagenen Protokoll benötigt jeder Teilnehmer ein Sende- und Empfangsschlüsselpaar für jede fremde TTP, die für einen Teilnehmer zuständig ist, mit dem er vertraulich kommunizieren möchte. Selbst wenn es je EU-Mitgliedsstaat nur eine einzige (nationale) TTP gäbe, wären das täglich 28 Schlüsselpaare je Bürger sowie weitere 28 Zertifikate (die allerdings sicherlich nicht alle täglich erzeugt würden).

Diese große Schlüsselzahl würde nicht nur zu einem erheblichen Kommunikationsaufwand zwischen Teilnehmern und der für sie zuständigen TTP führen, sondern insbesondere zu einer Vielzahl täglicher Schlüssel- und Zertifikatswechsel. Zur Beherrschbarkeit eines Key Recovery-Systems dieser Größenordnung mit erheblichen Verfügbarkeitsanforderungen gibt es bis heute keine Erfahrungen.[6]

4.2 Warum nicht Kerberos?

Da im vorgeschlagenen Protokoll die TTPs alle erforderlichen geheimen Schlüssel der Teilnehmer ihres Zuständigkeitsbereichs kennen und wiederum untereinander paarweise geheime (symmetrische) Schlüssel vereinbaren, würden symmetrische Schlüsselvereinbarungsprotokolle vollständig ausreichen. Das GCHQ-Protokoll ließe sich z.B. durch Kerberos ersetzen – ein auf symmetrischer Kryptographie beruhendes Sicherheitssystem, das 1988 am MIT entwickelt wurde [StNS_88] und die bewährten und gut untersuchten Schlüsselvereinbarungsprotokolle von Needham und Schröder verwendet [NeSc_78].

4.3 Ableitung der Schlüssel aus Identität

Wird ein geheimer Empfangsschlüssel eines Teilnehmers, den beide an einer grenzüberschreitenden Kommunikationsbeziehung beteiligten TTPs (und ggf. die Sicherheitsbehörden) kennen, kompromittiert, muß dieser ersetzt werden. Da aber der geheime Empfangsschlüssel eines Teilnehmers *A* von den beteiligten TTPs aus der Identität I_A des Teilnehmers und dem zwischen den TTPs vereinbarten geheimen Schlüssel *k* abgeleitet wird, muß entweder

- dieser geheime TTP-Schlüssel (und damit auch die geheimen Empfangsschlüssel aller anderen Teilnehmer beider TTPs!) oder
- die Identität des Teilnehmers

gewechselt werden.

Der jüngste Vorschlag der CESG versucht dieses Problem abzuschwächen, indem zusätzlich eine Schlüssel-ID in die Berechnung des geheimen Empfangsschlüssels eingeht, der in einem solchen Fall gewechselt werden muß [CESG_97].

Fazit

Zwar dürften die Kosten für den Aufbau und den Betrieb einer solchen Key Recovery-Infrastruktur deutlich unter denen des amerikanischen EES liegen, da das System ausschließlich in Software realisiert werden kann und daher keine aufwendige Personalisierung von Verschlüsselungschips erfordert. Die Kritik am EES gilt jedoch fast ausnahmslos auch für das GCHQ-Protokoll – abgesehen vielleicht von der Freiheit, einen Verschlüsselungsalgorithmus eigener Wahl verwenden zu können.

Wird im GCHQ-Protokoll der zwischen zwei TTPs vereinbarte geheime symmetrische Schlüssel kompromittiert oder hat eine Ermittlungsbehörde Zugriff auf diesen Schlüssel, ist technisch auch hier die Entschlüsselung über einen unbegrenzten Zeitraum möglich. Schlimmer noch: In dem vorgeschlagenen System ist bisher keine Zerlegung der geheimen Schlüssel und eine auf mehrere TTPs verteilte Hinterlegung der geheimen Schlüssel vorgesehen – anders als im EES wird dadurch jede TTP zum nationalen „big brother".

Und natürlich gilt auch für dieses Protokoll, daß Daten „vorverschlüsselt" werden können: Jeder Teilnehmer des Systems kann seine Nachrichten zunächst mit einem außerhalb des GCHQ-Protokolls vereinbarten Schlüssel verschlüsseln, und diese verschlüsselten Daten anschließend mit dem (regulären) Session Key *k* erneut verschlüsseln. Die Einführung eines solchen Protokolls würde daher wenigstens ein Verbot der Verwendung anderer Kryptoverfahren erfordern; eine Übertretung dieses Verbots wäre jedoch erst bei einer Abhörmaßnahme feststellbar.

Auch an der Durchsetzbarkeit einer solchen TTP-basierten Key Recovery-Lösung darf gezweifelt werden. Der amerikanische EES besaß immerhin noch die Chance, sich als preiswerter Standard-Kryptochip durchzusetzen. Ein System aber, das die Schlüsselaushandlung dominiert, ließe sich auf freiwilliger Basis kaum durchsetzen – schließlich hat der Teilnehmer nicht den geringsten Nutzen davon. Bliebe nur der obligatorische Weg – durch ein Verbot der Verschlüsselung mit anderen als den durch die (nationalen) TTPs generierten Schlüsseln. Es gibt allerdings – nicht zuletzt –

[5] Veranstaltungsbericht siehe Fox, DuD 9/1997, S. 555.

[6] Siehe auch Abelson, Anderson et.al., in diesem Heft.

gute Gründe, an der Verträglichkeit eines solchen Systems mit einer freiheitlichen Verfassung zu zweifeln.[7]

Anhang: Das DH-Protokoll

Das GCHQ-Protokoll basiert auf dem 1976 veröffentlichten Schlüsselaustauschverfahren von Diffie und Hellman (DH-Protokoll) [DiHe_76]. Dieses Verfahren erlaubt die Vereinbarung eines gemeinsamen geheimen Schlüssels über einen unsicheren Kanal.

Die Sicherheit des Diffie-Hellman-Protokolls (DH-Protokoll) basiert auf der mathematischen Schwierigkeit, *Diskrete Logarithmen* zu berechnen, d.h. die Lösung x einer Gleichung

$$y = g^x \bmod p$$

Dabei ist p eine sehr große Primzahl und g eine Primitivwurzel modulo p. Besitzt p mehr als 300 Dezimalstellen, kann nach heutiger Kenntnis davon ausgegangen werden, daß die Berechnung des Diskreten Logarithmus auch unter Aufbietung massiver Rechenressourcen einige Jahrhunderte dauern würde.

Das DH-Protokoll setzt die Vereinbarung zweier systemweit gültiger Parameter, den Werten für die Primitivwurzel g und den Modul p voraus. Wollen nun zwei Kommunikationsteilnehmer Alice (A) und Bob (B) einen gemeinsamen Schlüssel vereinbaren, wählen sie unabhängig voneinander jeweils eine zufällige Zahl x_A bzw. x_B (kleiner p-1) und berechnen daraus:

$$y_A = g^{x_A} \bmod p \text{ (Alice) bzw.}$$

$$y_B = g^{x_B} \bmod p \text{ (Bob)}$$

Diese Werte (y_A und y_B) tauschen sie nun gegenseitig aus. Dann können Alice und Bob einen gemeinsamen geheimen Schlüssel k_{AB} bestimmen:

$$k_{AB} = {y_B}^{x_A} \bmod p \text{ (Alice) bzw.}$$

$$k_{AB} = {y_A}^{x_B} \bmod p \text{ (Bob)}$$

Die Übertragung der Werte y_A und y_B muß dabei nicht geheim erfolgen, denn ein Abhörer könnte den Schlüssel k_{AB} nur dann bestimmen, wenn er einen der Diskreten Logarithmen von y_A oder y_B berechnen könnte.

Allerdings müssen y_A und y_B vor Verfälschung geschützt werden, da sonst ein Maskerade-Angriff (auch *Man-in-the-Middle*-Angriff genannt) möglich ist: Ein Angreifer könnte sich gegenüber Alice als Bob ausgeben und einen selbsterzeugten Wert y_B' an Alice senden.

Einen authentischen Austausch der Werte y_A und y_B ermöglichen Modifikationen des DH-Protokolls, wie z.B. das „*Station-to-Station*"-Protokoll (STS), in dem die Werte durch digitale Signaturen authentisiert werden [DiOW_92].

[7] Siehe dazu Bizer, DuD 4/1997, S. 203 ff.

Literatur

[AnRo_96] Anderson, Ross J.; Roe, Michael: *The GCHQ Protocol and Its Problems*. ftp.cl.cam.ac.uk/users/rja14/euroclipper.ps.Z, 1996.

[AnRo_97] Anderson, Ross J.; Roe, Michael: *The GCHQ Protocol and Its Problems*. In: In: Fumy, W. (Hrsg.): Proceedings of Eurocrypt '97, LNCS 1233, Springer, Berlin 1997, S. 134-148.

[CESG_96] CESG: *Securing Electronic Mail within HMG. Part I: Infrastructure and Protocol*. Draft C, 21.03.1996, Document T/3113TL/2776/11 (Internet: http://www.rdg.opengroup.org/public/tech/security/pki/casm/casm.htm).

[CESG_97] CESG: *An HMG Public Key Infrastructure to support Confidentiality.* CESG Infosec Memorandum No. 14, 04.02.1997, Document T/3522TL/2778/9 (Internet: http://www.rdg.opengroup.org/public/tech/security/pki/cki/mem14_10.pdf).

[DiHe_76] Diffie, Whitfield; Hellman, Martin E.: *New Directions in Cryptography*. IEEE Transactions on Information Theory, Vol. IT-22, No. 6, 1976, S. 644-654.

[DiOW_92] Diffie, Whitfield; Oorschot, Paul C. van; Wiener, Michael J.: *Authentication and Authenticated Key Exchange*. Designs, Codes & Cryptography, Nr. 2, 1992, S. 107-125.

[Fox_95] Fox, Dirk: *Zeitabhängiges Key Escrowing*. In: Trust Center. Proceedings der Arbeitskonferenz Trust Center 95, Verlag Vieweg, Braunschweig 1995, S. 232-245.

[Heus_95] Heuser, Ansgar: *Grenzüberschreitende Verschlüsselung und nationale Souveränität: ein Lösungsvorschlag*. In: Trust Center. Proceedings der Arbeitskonferenz Trust Center 95, Verlag Vieweg, Braunschweig 1995, S. 227-231.

[JeMW_95] Jefferies, Nigel; Mitchell, Chris; Walker, Michael: *A Proposed Architecture for Trusted Third Party Services*. In: Cryptography: Policy and Algorithms. LNCS 1029, Springer, Berlin 1995, S. 98-104.

[JeMW_96] Jefferies, Nigel; Mitchell, Chris; Walker, Michael: *Practical solutions to key escrow and regulatory aspects*. In: Proceedings der Public Key Solutions Conference, September 1996.

[Mitc_96] Mitchell, Chris J.: *The Royal Holloway TTP-based key escrow scheme*. ftp://ftp.dcs.rhbnc.ac.uk/pub/Chris.Mitchell/istr_a2.ps, 08.06.1996.

[NeSc_78] Needham, Roger M.; Schroeder, Michael D.: *Using Encryption for Authentication in Large Networks of Computers*. Communications of the ACM, Vol. 21, No. 12, 1978, S. 993-999.

[NIST_94] National Institute of Standards and Technology (NIST): *Escrowed Encryption Standard (EES)*. Federal Information Processing Standards Publication 185 (FIPS-PUB), 09.02.1994.

[Ruep_94] Rueppel, Rainer A.: *Clipper – Der Krypto-Konflikt am Beispiel der Amerikanischen ESCROW Technologie*. DuD 8/1994, S. 443-451.

[StNS_88] Steiner, Jennifer G.; Neumann, Clifford B.; Schiller, Jeffrey I.: *Kerberos: An Authentication Service for Open Network Systems*. USENIX, Winter '88, Dallas, Jan. 1988, S. 1-15.