Informatik Spektrum 22: 110–121 (1999)

Hauptbeitrag

Enterprise Key Recovery

Vertrauenswürdige Server mit skalierbarer Sicherheit zur Archivierung von Konzelationsschlüsseln

Hartmut Pohl, Dietrich Cerny

Zusammenfassung Im Electronic Commerce und in der digitalen Welt der zukünftigen globalen Informationsinfrastruktur (GII), bzw. dem Internet als deren Vorläufer, sollen Daten (Nachrichten und Dokumente) zwischen Kommunikationspartnern vertraulich, integer und rechtsverbindlich ausgetauscht und aufbewahrt werden können. Zur Erreichung des Sachziels 'Vertraulichkeit' werden Daten bei der Speicherung in unsicherer Umgebung und bei der Übertragung über unsichere Kanäle häufig von Endanwendern verschlüsselt. Dies setzt neben den erforderlichen Verschlüsselungsmechanismen geeignete Verfahren für das Management der Schlüssel voraus, die die Verfügbarkeit der verschlüsselt gespeicherten (oder übertragenen) Daten sicherstellen – auch wenn der originäre Besitzer des Schlüssels nicht verfügbar ist. Enterprise Key Recovery Server stellen Berechtigten bei Bedarf die Konzelationsschlüssel zur Entschlüsselung von Daten zur Verfügung. Ihre Funktionen werden zusammen mit angemessenen Sicherheitsmaßnahmen dargestellt. Für unterschiedliche Anforderungen an das Sicherheitsniveau wird eine skalierbare Sicherungsinfrastruktur für Enterprise Key Recovery Server vorgeschlagen. Die Nutzung von Enterprise Key Recovery Servern für das Management von Schlüsseln für den Nachrichtenaustausch und für digitale Signaturen ist nicht Thema dieser Arbeit. Erst der konsequente Einsatz von Key Recovery Servern sichert bei der Anwendung von Verschlüsselung die Vertraulichkeit und Verfügbarkeit von Daten und die Integrität der benutzten Schlüssel durchgängig ab. Key Recovery Server schließen damit eine empfindliche – bislang nicht genügend berücksichtigte – Sicherheitslücke in der Sicherheitsarchitektur von Unternehmen.

Schlüsselwörter Electronic commerce, Key recovery, Sicherheit, Sicherheitsarchitektur, Sicherheitsniveau, Skalierbarkeit, Unternehmen, Verschlüsselung

Summary In Electronic Commerce and in the digital world of the future Global Information Infrastructure (GII), respective the Internet as it´s predecessor, it is necessary that data (messages and documents) can be exchanged and stored between communicating partners confidentially, correctly and legally binding. To reach the objective of 'confidentiality', data will be encrypted by the enduser if they have to be stored in an insecure environment or have to be transmitted over insecure channels. In addition to the necessary cryprographic mechanisms, procedures for the management of keys are required which provide for the availability of the data which are stored (or transmitted) encrypted even if the original owner of the key is not available. On request, Enterprise Key Recovery Servers provide authorized users with the encryption key to decrypt data. The functionality of these servers is described together with adequate security measures. In order to support different security requirements a scalable security infrastructure for Enterprise Key Recovery Servers is proposed. The employment of Enterprise Key Recovery Servers for managing communication keys or keys for Digital Signatures is not part of this work. Only the systematic establishment of Key Recovery Servers provides for thourough confidentiality and availability of data and integrity of keys if encryption is used. Key Recovery Servers therefore close a severe security gap in the security architecture of enterprises, which has not been adequately addressed up to now.

Key words Business, Company, Electronic commerce, Encryption, Key recovery, Security, Security architecture, Security level

Computing Classification System D.4.6, E.5, H.2.0, K.4.4, K.6.5, K.6.m

Hartmut Pohl
Fachbereich Angewandte Informatik – Fachhochschule Rhein-Sieg, St. Augustin, ISIS InStitut für Informations Sicherheit, Max-Pechstein-Straße 4, D-50858 Köln,
Tel.: 0221 – 4847 – 526, Fax.:– 529, e-mail: Hartmut.Pohl@sang.net
Dietrich Cerny, 51147 Köln

1. Schlüsselmanagement, Sachziele und grundsätzliche Lösungsmöglichkeiten

Durch den zunehmenden Einsatz von kryptographischen Verfahren für den Schutz von Daten (Nachrichten, Dokumente) ergibt sich auch für Unternehmen das Problem des Schlüsselmanagements. Neben der Erzeugung, Überprüfung und Verteilung von Schlüsseln, ihrer Speicherung, Archivierung und Vernichtung [41, 45] wird insbesondere die Aufbewahrung der Schlüssel durch ihre steigende Anzahl komplexer. Vor allem die Notwendigkeit, verschlüsselte Daten – neben den Schlüsselbesitzern – auch anderen Berechtigten zeitnah zur Verfügung zu stellen, erfordert den Einsatz geeigneter Verfahren für das Management von Schlüsseln.

Im folgenden wird mit Enterprise Key Recovery Servern ein Ansatz vorgeschlagen, der die gewünschte Verfügbarkeit der Schlüssel sicherstellt.

Durch den Einsatz derartiger Key Recovery Server im Rahmen der Sicherheitsstrategie eines Unternehmens [38] und ihre Einbindung in seine Sicherheitsarchitektur wird ein höheres Sicherheitsniveau bei der Behandlung von Schlüsseln beim Unternehmen erreicht.

Derartige Key Recovery Server sind von Unternehmen, Institutionen und Einzelnen wiederholt gefordert [8, 10, 45, 25] und zuerst in den USA entwickelt worden; Standardisierungsvorschläge liegen vor [53].

Es sind auch andere Verfahren vorgeschlagen worden, die in jüngerer Zeit weniger beachtet wurden [u.a. 46, 62, 48, 3].

Die folgenden Betrachtungen beziehen sich ausschließlich auf (unternehmensinterne) Enterprise Key Recovery Server Produkte. Auf die nach wie vor aktuelle (politische) Diskussion über die Hinterlegung von kryptographischen Schlüsseln in der Folge des Escrowed Encryption Standard [1, 11, 14, 36, 37, 38, 39] wird hier nicht eingegangen.

1.1. Sicherheitsziel und -probleme

Zur Erreichung des Sachziels Vertraulichkeit bei der Speicherung und Übertragung von Daten werden Verschlüsselungsverfahren eingesetzt und es werden dazu - unabhängig vom benutzten Verschlüsselungsverfahren (symmetrisch „geheime" oder asymmetrisch „private") – Schlüssel benutzt; Zugriffsrechte auf diese Schlüssel besitzen ausschließlich Berechtigte.
Dabei ergeben sich die folgenden Sachziele für das Schlüsselmanagement:

- Sicherstellung der Verfügbarkeit der Schlüssel für Berechtigte:
  - Verfügbarkeit für den Endanwender zum Zeitpunkt des beabsichtigten Entschlüsselungsvorgangs.
  - Verfügbarkeit für andere Berechtigte (Kollegen und Vorgesetzte des Endanwenders) und damit Sperrung der Schlüssel für Unberechtigte (z.B. andere Kollegen, ausgeschiedene Endanwender).
- Sicherstellung der Verfügbarkeit der Schlüssel sowohl für den laufenden Betrieb als auch für archivierte Daten und das Backup.
- Integrität der gespeicherten Schlüssel und Übereinstimmung der gespeicherten Schlüssel mit den benutzten.

Der Besitzer des Schlüssels ist für seine ordnungsgemäße Behandlung und Aufbewahrung verantwortlich und hat ihn geheimzuhalten. Allerdings werden die in Unternehmen benutzten Schlüssel häufig nicht gemäß einer unternehmensspezifischen Sicherheitsstrategie gespeichert sondern nur entsprechend den subjektiven Vorstellungen der Endanwender. Damit wird jedoch kein einheitliches Sicherheitsniveau für die Schlüssel – und keine einheitliche Verfügbarkeit – erreicht. Dadurch kann die Situation eintreten, daß die mit diesen Schlüsseln verschlüsselt abgelegten Daten nicht mehr zur Verfügung stehen, weil der jeweilige Schlüssel verloren gegangen ist, entwendet wurde, absichtlich oder unabsichtlich gelöscht wurde, vom evtl. Trägermedium (z.B. Smartcard des Endanwenders) nicht mehr gelesen werden kann, vom Endanwender (widerrechtlich) zurückgehalten wird, von ihm verfälscht wurde oder weil der Endanwender nicht mehr im Unternehmen tätig ist.

Die Möglichkeit des Zugriffs auf den Schlüssel und damit auf die verschlüsselten Daten ist bisher abhängig von der Verfügbarkeit des Endanwenders. Allerdings ist dessen Verfügbarkeit z.B. auf Grund von Besprechungen, Reisen, Krankheit, Urlaub, Ausscheiden etc. temporär – auch im Rahmen vorgegebener Fristen – oder permanent – nicht immer gegeben.

Geeignete Verfahren zur Sicherstellung der Verfügbarkeit von Schlüsseln sind zwar vorhanden [13], werden aber bisher kaum angewandt.

1.2. Konzelations- und Signaturschlüssel

Schlüssel können nach ihren grundsätzlichen Funktionen als Konzelationsschlüssel und als Signaturschlüssel wie folgt unterschieden werden [21, 45, 49].

- Mit Konzelationsschlüsseln (encryption keys) – als symmetrische oder asymmetrische Verschlüsselung – wird das Sachziel Vertraulichkeit verfolgt.
- Mit Signaturschlüsseln (signature keys) werden in Anwendung des Verfahrens der digitalen Signatur die Sachziele Integrität und Authentizität verfolgt.

1.2.1. Konzelationsschlüssel

Als Konzelationsschlüssel werden im folgenden Schlüssel bezeichnet, mit deren Hilfe Daten in eine verschlüsselte Form überführt bzw. in den Klartext rücküberführt werden. Es handelt sich um Schlüssel, die zur Konzelation sowohl bei der Übertragung über unsichere Kanäle als auch bei der Speicherung in unsicherer Umgebung verwendet werden.

Als Maßnahme zur Erreichung der Vertraulichkeit bei der Übertragung bietet sich die (end-to-end) Konzelation an [67]. Allerdings ist die notwendige Schlüsselverteilung und der Schlüsselwechsel dann aufwendig, wenn mit vielen Partnern kommuniziert wird. Wegen des Risikos einer Kompromittierung des Konzelationsschlüssels sollte in diesen Fällen nicht ein und derselbe Konzelationsschlüssel benutzt werden. Damit stellt sich das Problem des Schlüsselmanagements. Soll ein gewisses Sicherheitsniveau erreicht werden, werden Konzelationsschlüssel häufig gewechselt (session key).

1.2.2. Signaturschlüssel

Als Signaturschlüssel wird der private Schlüssel eines asymmetrischen Verschlüsselungsverfahrens bezeichnet, der dazu dient, eine Nachricht digital zu signieren.

Mit der digitalen Signatur des Senders kann die Integrität und Authentizität von Daten nachgewiesen werden. Den Nachweis der Übereinstimmung der Identität eines Senders mit der von ihm benutzten digitalen Signatur erbringen Zertifizierungsstellen mit Hilfe von Zertifikaten. Dies sind von der Zertifizierungsstelle digital signierte Nachrichten, die mindestens Angaben zur Identität des Senders und seinen – zur Identifizierung der digitalen Signatur benötigten – öffentlichen Schlüssel enthalten [6, 40].

Signaturschlüssel werden in Unternehmen nicht grundsätzlich nur personenbezogen sondern häufig funktionsbezogen benutzt. Sie werden Rollen-orientiert nach standardisierten Benutzerprofilen für Funktionen (Geschäftsführer, Vorstand etc.) eingesetzt. In diesen Fällen muß die – Kontrollfunktionen ausübende – Instanz oder Rolle über den benutzten Signaturschlüssel verfügen können. Dazu ist es erforderlich, den

Signaturschlüssel so zu hinterlegen, daß er bei Bedarf zugreifbar ist. Es sind Modelle zur Bereitstellung von Signaturschlüsseln an ausgewählte Dritte mit festgelegten Rechten bekannt [5].

Diese Forderung nach funktionsbezogener Nutzung von Signaturschlüsseln ist umstritten; sie steht in Widerspruch zu der Forderung, die digitale Signatur eindeutig und unfälschbar an ein Individuum zu binden, um dem Risiko der Signatur durch Unberechtigte vorzubeugen. Sollen Rollen und Funktionen abgebildet werden, so können diese nämlich auch in Zertifikaten – auch z.B. zeitlich eingeschränkt – abgebildet werden. Es wird deshalb empfohlen, Signaturschlüssel ausschließlich personenbezogen zu verwenden [26, 67].

Signaturschlüssel können zwar auch als Konzelationsschlüssel eingesetzt werden [1]; allerdings kann die Kombination derart unterschiedlicher Funktionen nicht das Sicherheitsniveau eines Verfahrens erhöhen.

Im folgenden wird ausschließlich auf die Verarbeitung von Konzelationsschlüsseln eingegangen.

1.3. Vertrauenswürdige Instanzen

In Unternehmen fallen – entsprechend der jeweiligen Sicherheitsstrategie des Unternehmens – verschiedene sicherheitsrelevante Aufgaben an, die durch die im folgenden genannten vertrauenswürdigen Instanzen abgewickelt werden:

- **Zertifizierungsstellen:**
  Ausstellung von Zertifikaten zur Bestätigung des öffentlichen Schlüssels einer Identität zur Überprüfung einer digitalen Signatur.
- **Schlüsselmanagement-Instanzen (Key Management Center):**
  Generierung von Konzelationsschlüsseln und Signaturschlüsseln, deren Verteilung etc.
- **Enterprise Key Recovery Server:**
  Bereitstellung archivierter Konzelationsschlüssel.

Als vertrauenswürdig werden Instanzen dann bezeichnet, wenn sie technisch, organisatorisch und betrieblich so ausgestattet sind, daß sie ihre Aufgaben in einer vertrauenswürdigen und unabhängigen Weise durchführen. Vertrauenswürdige Instanzen werden auch als Trusted Third Party oder Trust Center bezeichnet. Als Trust Center sind insbesondere Zertifizierungsstellen bekannt geworden, die zur Verifizierung digitaler Signaturen öffentliche Schlüssel speichern und auf Anfrage vertrauenswürdig mit Hilfe von Zertifikaten mitteilen.

Als Enterprise Key Recovery Server werden vertrauenswürdige Instanzen bezeichnet, die eine vertrauenswürdige Wieder-Bereitstellung (Retrieval) von Konzelationsschlüsseln ermöglichen.

2. Funktionsweise von Enterprise Key Recovery Servern

Zur Erreichung der geforderten Verfügbarkeit von verschlüsselt gespeicherten Daten im Klartext müssen die zur Verschlüsselung benutzten Konzelationsschlüssel den Berechtigten im Bedarfsfall bereitgestellt werden können und die Berechtigten müssen diese Schlüssel nutzen können.

Enterprise Key Recovery Server[1] erfüllen diese Aufgabe indem sie die Konzelationsschlüssel den Berechtigten (zu Kontrollzwecken, bei Verlust des Schlüssels oder bei Nicht-Verfügbarkeit des Endanwenders) zur Verfügung stellen. Dazu besitzen sie geeignete Retrievalfunktionen, die zur Verhinderung unberechtigter Zugriffe von den übrigen Endanwender-Aktivitäten separiert sein müssen [51].

Konzelationsschlüssel können dabei nach unterschiedlichen Konzepten und auf unterschiedliche Art und Weise hinterlegt werden

Modelle für Key Recovery Server wurden bereits vorgeschlagen [31]. Inzwischen sind erste Produkte verfügbar [10, 42].

2.1. Hinterlegungskonzepte

Unter Hinterlegung (Escrowing) wird die Speicherung des benutzten Konzelationsschlüssels (oder einer Kopie) verstanden – außerhalb des eigentlichen Verschlüsselungsprozesses, also z.B. auf einem (anderen) Server, in einem anderen Prozeß oder mit den verschlüsselten Daten selbst.

Grundsätzlich können alle Arten von Schlüsseln, also Dateischlüssel (file keys), Geräteschlüssel (device keys), Grundschlüssel (master keys), Netzschlüssel (network keys), Sitzungsschlüssel (session keys) und Produkt-spezifische oder auch Benutzer-spezifische Schlüssel hinterlegt werden.

Es lassen sich vier Hinterlegungskonzepte (Escrowing) unterscheiden, das Archiv-Konzept und das Nachrichten-Konzept mit Speicher- und Kommunikationskonzept.

- **Archiv-Konzept**
  Vom Endanwender benutzte Konzelationsschlüssel werden in einem speziellen Key Recovery Center (vertrauenswürdige Instanz) hinterlegt – ggf. zusammen mit anderen identifizierenden Informationen. Bei diesem Konzept werden die verschlüsselten Daten getrennt von den Konzelationsschlüsseln gespeichert.
- **Nachrichten-Konzept**
  Vom Endanwender benutzte Konzelationsschlüssel werden (verschlüsselt) – ggf. zusammen mit anderen identifizierenden Informationen – zusammen mit den verschlüsselten Daten gespeichert (z.B. auf dem Server des Endanwenders) oder übertragen. Bei diesem Konzept werden die Schlüssel nicht in einer vertrauenswürdigen Instanz wie einem Key Recovery Center zur Hinterlegung gespeichert.
  Die Nachrichten-Konzept wird auch als Recovery Key, Message Recovery oder Key Encapsulation [13, 22] bezeichnet.
  Beim Nachrichten-Konzept werden zur Speicherung der Schlüssel die beiden Konzepte Speicherkonzept und Kommunikationskonzept unterschieden.
- **Speicherkonzept**
  Die verschlüsselten Daten werden zusammen mit den zugehörigen Konzelationsschlüsseln in einem Datenspeicher (Server) des Endanwenders gespeichert.

[1] Die Terminologie ist uneinheitlich und nicht genormt [52]. Die Begriffe Enterprise Key Recovery Server oder Key Recovery Center oder allgemein Recovery Center (RC) oder Self-Escrow (SE) werden synonym benutzt.

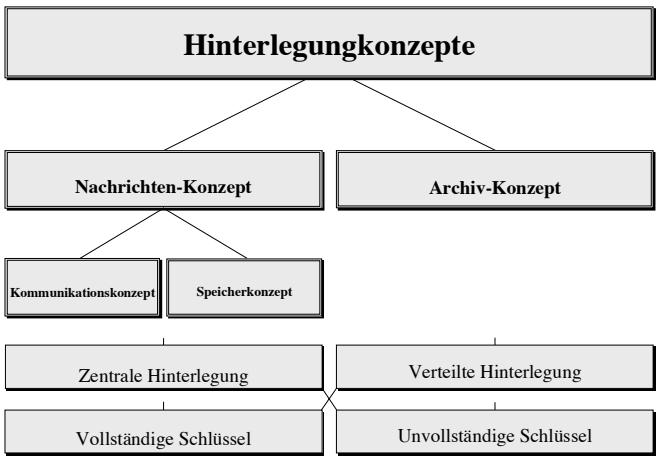

Abb. 1 Gliederung der Hinterlegungskonzepte [2]

– **Kommunikationskonzept**
  Die verschlüsselten Daten (z.B. e-mails) werden zusammen mit den zugehörigen Konzelationsschlüsseln übertragen. Es ist nicht festgelegt, ob der Sender die Daten in Klartext oder verschlüsselt aufbewahrt und/oder der Empfänger. Der benutzte Schlüssel wird nur übertragen, er wird nicht in einem Key Recovery Center hinterlegt. Ein Retrieval des benutzten Schlüssels und/oder der Daten ist in diesem Fall daher nur möglich, wenn der Inhalt eines Übertragungsvor-gangs vollständig kopiert wurde, um im Bedarfsfall den Schlüssel zusammen mit den benötigten verschlüsselten Daten zur Verfügung zu haben.

2.2. Hinterlegungsarten

Unter dem Aspekt des bestmöglichen Schutzes der Konzelationsschlüssel werden unterschiedliche Hinterlegungsarten von Schlüsseln angegeben.

– **Zentrale Hinterlegung (escrow center)**
  Der Schlüssel wird auf einem (einzigen) Key Recovery Server gespeichert bzw. in einer einzigen Nachricht übertragen.
– **Verteilte Hinterlegung (split key system)**
  Der Schlüssel wird geteilt und die Teile werden auf verschiedenen Key Recovery Server gespeichert bzw. in mehreren Nachrichten übertragen. Schlüssel können derart geteilt werden, daß die erneute Zusammenfügung der Teilschlüssel aller Key Recovery Server den Schlüssel ergibt oder so, daß nur ein Teil der Key Recovery Server beteiligt wird (split key, secret sharing, threshold scheme). Durch die Hinterlegung bei mehreren Recovery Servern kann das Mißbrauchsrisiko gesenkt werden, da ein Angreifer einen erhöhten Aufwand treiben müßte, um den Gesamtschlüssel zu erhalten. Bei der Hinterlegung bei nur einem Teil der installierten Key Recovery Server wird das Sicherheitsniveau erhöht, weil ein Angreifer nicht die tatsächlich beteiligten Key Recovery Server kennt. Eventuelle Plausibilitätsprüfungen sind wegen der Verteilung allerdings erschwert. Verfahren mit verteilter Hinterlegung und Verifizierung wurden vorgeschlagen [34].
– **Vollständig hinterlegte Schlüssel (full escrow)**
  Der Schlüssel wird in voller Länge hinterlegt.
– **Unvollständig hinterlegte Schlüssel (partial escrowing)**
  Der Schlüssel wird unvollständig hinterlegt. Beim Retrieval des jeweiligen Schlüssels, wird der nicht-hinterlegte Teil des Schlüssels durch eine sog. brute force attack bestimmt [47, 64 sowie 2, 12]. Allerdings ist der Aufwand dieser Hinterlegungsart für den Berechtigten gleich hoch wie für den Angreifer.

Die Hinterlegungsart 'vollständig hinterlegter Schlüssel' erscheint nützlich, solange die hinterlegten Schlüssel häufig wieder bereitgestellt werden müssen und damit die Anzahl der Retrieval-Fälle hoch ist. Die Hinterlegungsart 'unvollständig hinterlegte Schlüssel' kann dann sinnvoll sein, wenn die Key Recovery Komponente selten in Anspruch genommen wird; dann lohnt sich der seltene Aufwand im Vergleich zum stark erhöhten Sicherheitsniveau.

2.3. Komponenten von Key Recovery Systemen

Erste Ansätze einer differenzierenden Beschreibung von Key Recovery Systemen sind veröffentlicht worden [13, 22, 33]. Im folgenden sollen die Funktionsprinzipien von Key Recovery Systemen dargestellt werden, die nach dem Nachrichtenkonzept – speziell Speicherkonzept – arbeiten (vgl. Abb. 4: 'Funktionales Modell von Enterprise Key Recovery').

Ein Key Recovery System besteht aus zwei logischen Komponenten, die unter Sicherheitsaspekten zweckmäßigerweise in unterschiedlichen Funktionseinheiten realisiert sein sollten [20, 22, 66 sowie 54 – 62]: Aus der Schlüsselkomponente des Endanwenders und der Key Recovery Komponente. Diese Komponenten sind in der Abb. 4: 'Funktionales Modell von Enterprise Key Recovery' dargestellt. Jede dieser Komponenten enthält sog. Agenten, die für die Aufgabenwahrnehmung und für das Zusammenwirken der Komponenten zuständig sind.

Stand der Technik ist die Realisierung der Key Recovery Komponente in einem Key Recovery Server.

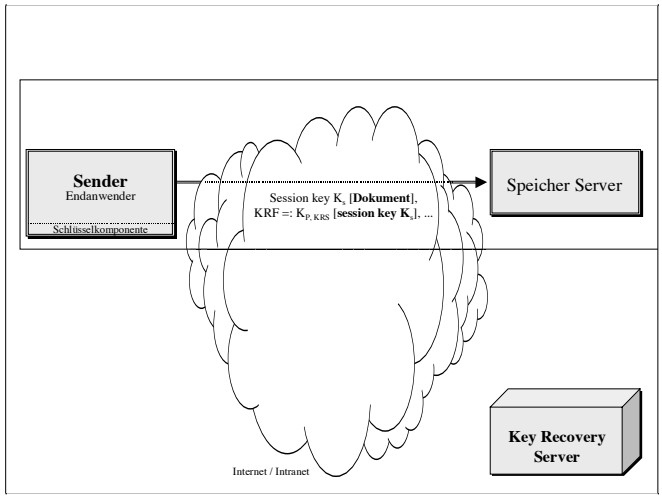

Abb. 2 Enterprise Key Recovery: Verschlüsseltes Speichern benutzter Konzelationsschlüssesel

[2] Legende zu den Abbildungen

Übertragung von Kontroll- und Steuerinformation
Übertragung von Daten
Übertragung von Schlüsseln

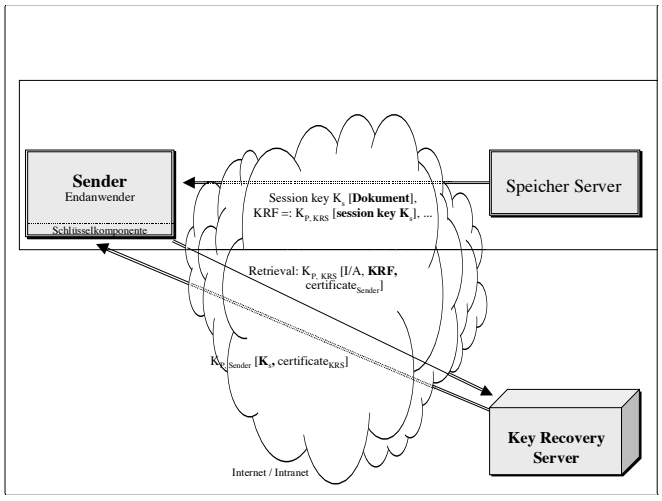

Abb. 3 Enterprise Key Recovery: Retrieval verschlüsselt gespeicherter Konzelationsschlüssel

2.3.1. Schlüsselkomponente des Endanwenders – SKE

Die Schlüsselkomponente (Hardware und/oder Software) ist im System des Endanwenders installiert. Sie übt – neben der Anmeldung des Endanwenders bei der Key Recovery Komponente – die folgenden Funktionen aus:

- Konzelation der Daten (und ihre Entschlüsselung).
- Übermittlung des zur Konzelation benutzten Schlüssels an die Key Recovery Komponente. Die Übermittlung kann zu unterschiedlichen Zeitpunkten erfolgen, in der jeweiligen Session, sporadisch oder zu festgelegten Zeiten – z.B. zum Zeitpunkt des Schlüsselwechsels.

Zur Durchführung ihrer Aufgaben kann die Schlüsselkomponente die folgenden – in Kap. 2.4 'Zusammenwirken der Komponenten' erläuterten – Agenten enthalten: Anmeldeagent, Key Recovery Feld Generator, Übertragungsagent, Konzelationsagent.

2.3.2. Key Recovery Komponente – KRK

Diese Komponente hat die Aufgabe der

- Verschlüsselten Speicherung der von der Schlüsselkomponente des Endanwenders übertragenen Schlüssel sowie
- Speicherung der zur Entschlüsselung benötigten weiteren Informationen (zur Identifizierung und Authentifizierung der Berechtigten). Diese zur Entschlüsselung benötigten weiteren Informationen sind – zusammen mit dem Schlüssel – in einem sog. Key Recovery Feld (KRF) abgespeichert [11, 54 – 62]; vgl. Abb. 5: Mögliche Inhalte eines Key Recovery Feldes (KRF)'.

Zur Durchführung ihrer Aufgaben kann die Key Recovery Komponente einen Registrierungs- und einen Retrievalagenten enthalten.

2.4. Zusammenwirken der Komponenten von Key Recovery Systemen

Das Zusammenwirken der Komponenten und die Kommunikation zwischen den Komponenten wird durch die Agenten realisiert. Die Agenten werden im folgenden beschrieben.

Anmeldeagent
Der Anmeldeagent ist eine Funktionseinheit der Schlüsselkomponente des Endanwenders zur Anmeldung beim Registrierungsagenten der Key Recovery Komponente.

Vor der ersten Nutzung der Key Recovery Komponente muß sich der Endanwender mit Hilfe des Anmeldeagenten seiner Schlüsselkomponente gegenüber dem Registrie-

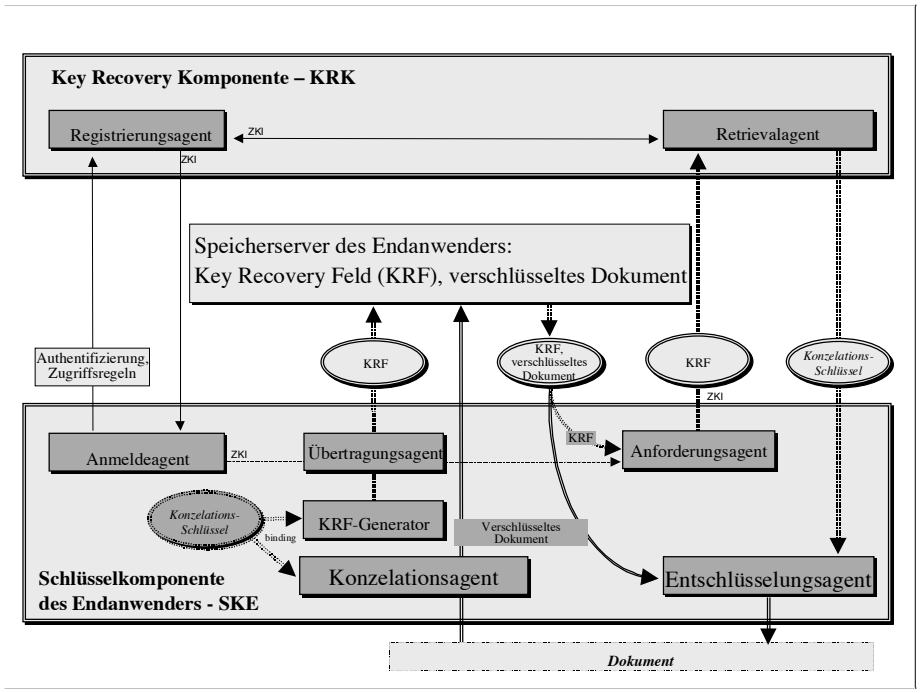

Abb. 4 Funktionales Modell von Enterprise Key Recovery

Abb. 5 Mögliche Inhalte eines Key Recovery Feldes (KRF)

rungsagenten mit geeigneten Daten wie einem Zertifikat (z.B. mit Vor- und Nachname, Geburtsdatum und -ort, Adresse, Abrechnungsart etc.) und seiner digitalen Signatur anmelden, identifizieren und authentifizieren [40].

Zusätzlich zu den Identifizierungs-/Authentifizierungsinformationen gibt der Endanwender bei der Anmeldung alle aus seiner Sicht angemessenen Regeln für das Zugriffskontrollsystem des Key Recovery Servers an und legt damit fest, welche anderen Endanwender zum Zugriff auf den Schlüssel und damit auf die Daten berechtigt sein sollen. Diese Menge der Zugriffskontrollregeln wird hier als Zugriffskontroll-Regelsatz bezeichnet. Die Anmeldung ist für jede – hinsichtlich des Zugriffskontroll-Regelsatzes einheitlich zu behandelnde – Menge von Schlüsseln zu wiederholen.

Registrierungsagent
Der Registrierungsagent ist eine Funktionseinheit der Key Recovery Komponente des Endanwenders zur Registrierung der Anmeldung durch die Schlüsselkomponente des Endanwenders.

Der Registrierungsagent überprüft die Identifizierungs-/Authentifizierungsinformation eines Endanwenders, speichert sie und stellt sie für das Retrieval zur Verfügung.

Die Key Recovery Komponente wiederholt die Identifizierung und Authentifizierung des Endanwenders bei jeder Speicherung eines Schlüssels, um den übersandten Schlüssel wieder zuordnen zu können.

Der Registrierungsagent sendet dem Anmeldeagenten die Identifizierungs-/Authentifizierungsinformationen zusammen mit dem Zugriffskontroll-Regelsatz als sog. Zugriffskontroll-Information (ZKI) zurück zur Verwendung als Identifikationsnachweis bei einem eventuellen Retrieval des Schlüssels.

Zugriffskontroll-Information – ZKI
Die Zugriffskontroll-Information kann u.a. die folgenden Felder enthalten.
- Art, Name und Version des Archivprodukts – oder Identifier dazu. Struktur und Aufbau des ZKI.
- Kennzeichnung des Endanwenders (z.B. Name, Adresse, Identifizierungs- und Authentifizierungsinformation wie Paßworte, biometrische Merkmale, Lizenznummer der Schlüsselkomponente, eine bei der Registrierung vergebene Nummer) oder Identifier.
- Benutzte Key Recovery Server (Name, Adresse – oder auch URL – des Servers). Der Eintrag ist verzichtbar, wenn nur ein einziger Server genutzt wird.
- Hinweise (Identifier) auf früher übersandte ZKI, die ggf. durch dieses ersetzt werden.
  Laufende Nummer des zugehörigen Key Recovery Felds oder Identifier zu seiner Kennzeichnung.
- Regelsatz für die Zugriffskontrolle oder Identifier.
- Laufende Nummer des Regelsatzes zu Prüfzwecken.
- Angaben zur Gültigkeit dieses ZKI wie Zeitpunkt, Zeitintervall oder logische Abhängigkeiten.
- Zeitstempel [45] und digitale Signatur des Endanwenders.

Generator des Key Recovery Felds
Der Generator des Key Recovery Felds generiert im Fall der Konzelation von Daten ein Key Recovery Feld (evtl. verschlüsselt) und trägt den benutzten Konzelationsschlüssel zusammen mit anderen identifizierenden Informationen z.B. über das benutzte Key Recovery Produkt, die Version, die Zugriffskontroll-Information etc. in das Key Recovery Feld ein. Das KRF enthält also die relevante Information für das Retrieval. Das Key Recovery Feld enthält weiterhin einen Zeitstempel und eine digitale Signatur des Endanwenders.

Das Key Recovery Feld kann unverschlüsselt sein und damit lesbar; es kann vom Empfänger zu Prüfzwecken (Integrität, Authentizität) genutzt werden. Die Vertraulichkeit des KRF ist nur durch die Zugriffskontrolle des Speicherservers des Endanwenders gewährleistet.

Stand der Technik ist eine Verschlüsselung des Konzelationsschlüssels durch den Generator des Key Recovery Felds. Das Feld könnte mit dem öffentlichen Schlüssel des Retrievalagenten des KRF verschlüsselt werden. Über den Konzelationsschlüssel hinaus könnten auch weitere Teile des KRF verschlüsselt werden. Davon wird im folgenden ausgegangen.

Key Recovery Feld
Das Key Recovery Feld kann die folgenden Informationen enthalten.
- Art, Name und Version des Key Recovery Server Produkts – oder Identifier dazu. Struktur und Aufbau des KRF.
- Kennzeichnung des Endanwenders (z.B. Name, Adresse, Lizenznummer der Schlüsselkomponente, eine bei der Registrierung vergebene Nummer) oder Identifier.
- Angaben zur Gültigkeit dieses KRF: Laufende Nummer oder Identifier der Session, in der der Schlüssel benutzt wurde. Ggf. werden auch in einer Session mehrere Schlüssel genutzt. Es werden dann mehrere KRF generiert.
- Benutzter Key Recovery Server (Name, Adresse (URL) des Key Recovery Servers). Der Eintrag ist verzichtbar, wenn nur ein einziger Server genutzt wird.

– Adressierte Kommunikationspartner: Name, Adresse, Registrierungsnummer und Versionsnummer der Schlüsselkomponenten.
– Schlüssel (session key) oder Identifier oder Adresse (URL).
– Parameter des Schlüssels wie eine laufende Nummer, Länge in Bit, bei split key Konzepten Anzahl der Teile mit Teilenummer, benutzter Algorithmus, Implementierung, Produkt, Version, Gültigkeitszeitpunkt oder Dauer, Archivierungszeitraum.
– Master Key des gesamten Verfahrens: Konzelationsschlüssel dieses Schlüssels oder Identifier wie laufende Nummer, Adresse, Länge in Bit, benutzter Algorithmus, Produkt, Version, Gültigkeitszeitpunkt oder Dauer, Archivierungszeitraum.
– Zugehörige Zugriffskontroll-Information oder Identifier zu seiner Kennzeichnung zur Identifizierung und Authentifizierung der Retrieval-Berechtigten.
– Identifier zur Information über erkannte Manipulationen an der Schlüsselkomponente des Endanwenders (KRF Verifizierungsfeld).
– Zeitstempel und digitale Signatur des Endanwenders.

Übertragungsagent
Der Übertragungsagent (Funktionseinheit der Schlüsselkomponente des Endanwenders) überträgt das KRF zur Key Recovery Komponente KRK für ein eventuelles Retrieval des Schlüssels.

Nach Eingang des Key Recovery Felds und nach Integritätsprüfungen meldet er den korrekten Eingang des Key Recovery Felds an den Konzelationsagenten der Schlüsselkomponente und gibt damit die Nutzung dieses Konzelationsschlüssels frei.

Konzelationsagent
Der Konzelationsagent ist eine Funktionseinheit der Schlüsselkomponente des Endanwenders, der die Daten des Endanwenders verschlüsselt.

Nach Eingang der Rückmeldung vom Übertragungsagenten, daß das Key Recovery Feld korrekt eingegangen ist, verschlüsselt der Konzelationsagent die Daten mit dem freigegebenen Schlüssel; es kann anschließend gespeichert werden.

Anforderungsagent
Der Anforderungsagent ist eine Funktionseinheit der Schlüsselkomponente des Endanwenders zur Entgegennahme der Anforderung, Überprüfung der Integrität sowie der Authentizität des Anfordernden und Weiterleitung der Anforderung an den Retrievalagenten der Key Recovery Komponente.

Benötigt der Endanwender – oder ein Dritter – die Daten erneut, so fordert er mit dem Anforderungsagenten den Schlüssel beim Retrievalagenten der Key Recovery Komponente an; dabei identifiziert er sich mit der zu dem benötigten Konzelationsschlüssel gehörenden Zugriffskontroll-Information.

Retrievalagent
Der Retrievalagent ist eine Funktionseinheit der Key Recovery Komponente zur Wieder-Bereitstellung der Konzelationsschlüssel aus den Key Recovery Feldern.

Der Retrievalagent überprüft die Zugriffskontroll-Information und stellt den zugehörigen zur Entschlüsselung benötigten Konzelationsschlüssel bereit, indem er ihn dem zugehörigen KRF entnimmt und entschlüsselt. Dazu wird bei symmetrischer Verschlüsselung ein – nur dem Retrievalagenten bekannter – Grundschlüssel (master key) benötigt oder bei asymmetrischer Verschlüsselung der private Schlüssel des Retrievalagenten.

Der Retrievalagent setzt im Falle des split key Verfahrens (mehrere Key Recovery Felder) die Schlüsselteile auch wieder zusammen.

Bei unvollständig hinterlegten Schlüsseln (partial key escrowing) muß der Retrievalagent den nicht-hinterlegten Teil des Schlüssels durch ein Verfahren zur Schlüsselbestimmung generieren, das einer brute force attack entspricht.

Entschlüsselungsagent
Der Entschlüsselungsagent ist eine Funktionseinheit der Schlüsselkomponente des Endanwenders zur Entschlüsselung benötigter Daten mit dem vom Retrievalagenten bereitgestellten Konzelationsschlüssel.

Der Entschlüsselungsagent erhält den (entschlüsselten) Konzelationsschlüssel vom Retrievalagenten über den Anforderungsagenten.

Werden von dem Besitzer der Daten, einem anderen Endanwender oder einem Dritten die verschlüsselt abgelegten Daten benötigt, so identifiziert dieser sich der Anforderungsagent der Schlüsselkomponente des Endanwenders mit seiner digitalen Signatur und einem Zertifikat als Berechtigter und fordert den zugehörigen Konzelationsschlüssel an.

3. Skalierbare Sicherheitsinfrastruktur

Enterprise Key Recovery Server verarbeiten mit den Konzelationsschlüsseln wertvolle Daten. Es ist daher notwendig, daß diese gespeicherten Schlüssel sehr stark geschützt werden. Dies kann nur durch die Realisierung der folgenden Maßnahmen in den Komponenten der Key Recovery Systeme erreicht werden.

3.1. Sicherstellung der Integrität der Komponenten

Es liegen Vorschläge vor, mit deren Hilfe die Manipulation von Hardware- oder Software-basierten Key Recovery Systemen mit dem Ziel einer Umgehung des Hinterlegungsverfahrens erkannt und verhindert werden kann [65]. Dies gilt für Manipulationen an einer einzigen Komponente – insbesondere der Schlüsselkomponente des Endanwenders. Dies gilt auch für Manipulationen an zwei Komponenten (wie den beiden Schlüsselkomponenten von zwei Kommunikationspartnern). Integritätsverletzungen der einzelnen Komponenten des Key Recovery Systems können durch gegenseitige Prüfung festgestellt werden.

Mit dieser Integritätsprüfung können Manipulationen an einzelnen Komponenten erkannt werden – aber nicht eine Manipulation aller Komponenten inklusive der Prüffunktion. Eine Integritätsverletzung aller Komponenten kann nur durch Integritätsprüfung aller Komponenten erkannt werden. Eine solche Integritätsprüfung ist möglich:

– **Integritätsprüfung durch die Hardware** oder Firmware des Key Recovery Systems: Unter der Voraussetzung der manipulationssicheren Implementierung (tamper-resistant box) kann sichergestellt werden, daß auf einer bestimmten Hardware integre Softwarekomponenten ablaufen (controlled execution). Dies gilt für Softwarekomponenten wie das Betriebssystem, Datenbanksysteme bis hin zu allen Anwendungen. Durch die Möglichkeit kontinuierlicher und funktionsbezogener Prüfungen kann eine Manipulation der Komponenten des Key Recovery Servers allerdings praktisch ausgeschlossen werden. Insbesondere müßte dazu der Informationsfluß zu und von der Hardware vollständig überwacht werden [65].
– **Integritätsprüfung über ein Netz:** Integritätsverletzungen der Softwarekomponenten können von außerhalb des Key Recovery Servers durch Prüfung der Komponenten erkannt werden. Allerdings sind Manipulationen der Komponenten im Key Recovery Server möglich, die ein korrektes Ergebnis der Integritätsprüfung der Software vortäuschen; daher sollte die Integrität der Hardware mit geprüft werden.

Unberücksichtigt bleiben muß hier der Aspekt der Implementierung undokumentierter Funktionen bereits bei der Softwareerstellung; derartige Schwachstellen können im Evaluierungsverfahren [9, 15] erkannt werden.

Bei der Implementierung und Installation einer Anwendung muß von einem Tool vertrauenswürdig sichergestellt werden, daß die Key Recovery Funktion genutzt wird.

3.1.1.Nutzung von Verzeichnissen (directories)

Mit der Verschlüsselung von Daten wird vorrangig das Sachziel 'Vertraulichkeit' erreicht. Um zu überprüfen, ob die gespeicherten Daten wieder unverändert gelesen wurden (Sachziel: Integrität), speichert der Endanwender zusätzlich seine digitale Signatur mit den Daten ab. Um bei Nicht-Verfügbarkeit des Mitarbeiters dem Unternehmen eine Integritätsprüfung zu ermöglichen, muß ihm der öffentliche Schlüssel des Mitarbeiters zur Verfügung stehen. Die öffentlichen Schlüssel der Mitarbeiter werden in einem unternehmenseigenen Verzeichnis (directory) gespeichert und von diesem bereitgestellt [23, 24].

3.1.2.Schutz der private Schlüssel von Key Recovery Servern

Werden die benutzten Konzelationsschlüssel vom Endanwender mit dem öffentlichen Schlüssel des Key Recovery Servers verschlüsselt abgespeichert, sind sie (nur) mit dem privaten Schlüssel des Key Recovery Servers zu entschlüsseln. Wird der private Schlüssel des Key Recovery Servers kompromittiert, so sind alle im Unternehmen gespeicherten Konzelationsschlüssel kompromittiert. Der private Schlüssel des Key Recovery Servers muß also gegen unberechtigten Zugriff geschützt werden: Das Problem des Schutzes der Schlüssel wird ersetzt durch die Aufgabe, den privaten Schlüssel des Key Recovery Servers gegen unberechtigte Kenntnisnahme zu schützen. Der private Schlüssel könnte in einem anderen Key Recovery Server – dem Sicherheitsserver des Unternehmens – hinterlegt werden.

3.1.3.Validierung des Key Recovery Feldes

Das Key Recovery Feld muß insgesamt und alle Felder des Key Recovery Feldes müssen einzeln hinsichtlich ihrer Integrität überprüft werden.
Gegebenenfalls müssen auch (benutzerbezogen) weitere Felder ergänzt werden. So sind die folgenden Felder denkbar:
– Hierarchische oder kategoriale Einstufung [38] des Verschlüsselungsalgorithmus.
– Gesetzeskonformität des Produkts.

3.1.4.Kontrolle des Informationsflusses

Alle Agenten des Key Recovery Systems überprüfen die eingehenden Daten anderer Komponenten und Agenten und melden sich gegenseitig den korrekten Eingang; erst danach werden weitere Aktivitäten eingeleitet.

So überprüft der Übertragungsagent der Schlüsselkomponente des Endanwenders den benutzten Konzelationsschlüssel hinsichtlich Integrität und Vollständigkeit vor der Übertragung an den Speicherserver des Endanwenders und vor der Verschlüsselung der Daten durch den Konzelationsagenten. Anderenfalls, wäre eine Speicherung ohne oder mit einem anderen als dem zur Konzelation benutzten Schlüssel nicht auszuschließen.

3.2.Skalierbarkeit: Stufen des Sicherheitsniveaus

Im folgenden sollen beispielhaft einige Sicherheitsstufen für den Einsatz von Key Recovery Servern in Unternehmen vorgeschlagen werden [44].

Der Ansatz geht davon aus, daß der Widerstandswert des Key Recovery Verfahrens mit steigender Sicherheitsstufe zunimmt. Mit einer solchen Skala von Sicherheitsstufen läßt sich ein Key Recovery Verfahren an unterschiedliche Sicherheitsanforderungen anpassen. Im Falle der Realisierung muß anhand einer vollständigen Risikoanalyse die – entsprechend der Sicherheitsstrategie des Unternehmens aktuell angemessene – Sicherheitsstufe für den Key Recovery Server festgelegt werden.

In der Tabelle 1 'Skalierbares Sicherheitsniveau in Unternehmen (Levels of Trust)' werden beispielhaft einige Sicherheitsstrategien dargestellt sowie eine als Maßnahme bezeichnete Beschreibung der jeweiligen Strategie und das verbleibende Restrisiko. Die Darstellung der höheren Stufen erfolgt so, daß nur die – im Vergleich zu den niedrigeren Stufen – zusätzlichen Sicherheitsmaßnahmen aufgeführt werden. Hier sollen nur einige Aspekte der ansonsten selbsterklärenden Sicherheitsstufen 7 und 8 ausgeführt werden.

In der Sicherheitsstufe 7 wird durch die Forderung nach verteilten Key Recovery Servern eine funktionierende Key Recovery Infrastruktur im Unternehmen gefordert. Unter Infrastruktur werden hier nur die technischen und organisatorischen Einrichtungen verstanden, die zur Verarbeitung (insbesondere Speicherung) von Konzelationsschlüsseln benutzt werden.

Werden bei einem Unternehmen mehrere Key Recovery Server installiert, muß vereinbart werden, welche – ggf. unterschiedlichen und/oder sich ergänzenden – Funktionen die

Tabelle 1 Skalierbares Sicherheitsniveau in Unternehmen (Levels of Trust)

Inhalt der Sicherheitsstrategie	Maßnahme	Verbleibendes Risiko
1. Daten werden offen (**unverschlüsselt**) gespeichert und übertragen.	**Sensibilisierung** für die Risiken der Informationsverarbeitung.	**Mit- und Abhören** sowie Ändern der Daten. Die Gesamtsicherheit hängt ab vom Sicherheitsniveau der benutzten Netze.
2. Das Unternehmen benutzt einem **einzigen Konzelationsschlüssel**. Endanwender speichern ihn nach eigenen **Sicherheitsvorstellungen**.	Ein **Schlüssel-Generator** generiert, speichert und verteilt den Konzelationsschlüssel. Bei Bedarf kann er vom Generator bezogen werden oder dem Back-up der Schlüssels entnommen werden.	Wird der Schlüssel des Unternehmens kompromittiert, so lassen sich **alle** Nachrichten und Dokumente des Unternehmens entschlüsseln, die jemals gespeichert oder übertragen wurden. Die Gesamtsicherheit hängt ab vom Sicherheitsniveau des Schlüssel-Generators.
3. **Unterschiedliche** Konzelationsschlüssel für die Endanwender.	**Diese** Konzelationsschlüssel werden vom Schlüssel-Generator generiert, gespeichert und verteilt.	Wird der Schlüssel eines Endanwenders kompromittiert, so lassen sich alle Nachrichten und Dokumente des Endanwenders entschlüsseln, die dieser Endanwender jemals verarbeitet hat. Es können auch zukünftig die verarbeiteten Dokumente entschlüsselt werden – sofern der Schlüssel nicht gewechselt wird. Das **Sicherheitsniveau** ist höher als bei der Lösung mit einem einzigen Unternehmensschlüssel.
4. Einsatz von **session keys**. Speicherung in einer speziellen Funktionseinheit (**Schlüssel–Archiv**).	Die session keys werden in einem **Schlüssel–Archiv** gespeichert. Bei Bedarf können sie Berechtigte vom Key Recovery Server beziehen.	Wird das (zentrale) Schlüssel–Archiv kompromittiert, so fallen **alle** Schlüssel des Unternehmens dem Angreifer in die Hände und es lassen sich **alle** Nachrichten und Dokumente des Unternehmens entschlüsseln, die jemals gespeichert oder übertragen wurden und werden. Die Gesamtsicherheit hängt ab vom Sicherheitsniveau des zentralen Schlüssel–Archivs.
5. **Verteilte** und/oder **unvollständige** Speicherung der Konzelationsschlüssel.	**Split Key**: Teile der Konzelationsschlüssel werden auf mehrere Schlüssel–Archive verteilt. Unvollständig gespeicherte Konzelationsschlüssel können nicht ausgelesen werden. Vielmehr muß zur Bestimmung des vollständigen Schlüssels eine 'brute force attack' vorgenommen werden.	Angreifer muß **alle** Schlüssel–Archive angreifen oder Insiderwissen besitzen. Geringes verbleibendes Risiko. Allerdings muß diese 'brute force attack' auch bei berechtigtem Bedarf vorgenommen werden.
6. **Verschlüsselte** Speicherung der Konzelationsschlüssel im Schlüssel–Archiv.	Die Schlüssel werden im Schlüssel–Archiv mit dem public key des Schlüssel–Archivs **verschlüsselt** gespeichert. Bei Bedarf kann er vom Schlüssel–Archiv bezogen werden, das ihn mit seinem private key entschlüsselt bereitstellt..	Wird der private key des Schlüssel–Archivs kompromittiert, so können **alle** gespeicherten Schlüssel entschlüsselt und ausgelesen werden und damit alle (gespeicherten und übertragenen) Dokumente entschlüsselt werden. Die Gesamtsicherheit hängt ab vom Sicherheitsniveau des Schlüssel–Archivs. Es wird ein höheres Niveau gegenüber vorangehenden Lösung erreicht.
7. **Verteilte Schlüssel–Archive** mit einem **Master Schlüssel–Archiv**: Sicherungsinfrastruktur.	Einsatz **dezentrale** Schlüssel–Archive und verschlüsselte Speicherung der private keys dieser Schlüssel–Archive in einem **Master Schlüssel–Archiv**.	Hohe Gesamtsicherheit durch **dezentrale Schlüssel–Archive**. Daneben hängt das Gesamtsicherheitsniveau ab vom Master Schlüssel–Archiv.
8. **Enterprise Key Recovery Server (EKRS).**	Enterprise Key Recovery Server stellen dem Endanwender ihren public key public key zur Verschlüsselung benutzter Konzelationsschlüssel zur Verfügung. Endanwender legen das Sicherheitsniveau (mit den Zugriffskontrollmaßnahmen) selbst fest.	Höchstes Sicherheitsniveau durch: 1. Einsatz von Key Recovery Servern und damit generellen **Verzicht auf Speicherung** der (verschlüsselten oder unverschlüsselten) Konzelationsschlüssel oder auch nur von Informationen über Konzelationsschlüssel. 2. **Informationswert-abhängige** Sicherheitsmaßnahmen auf den Servern der Endanwender, auf denen Konzelationsschlüssel gespeichert sind – unabhängig vom Sicherheitsniveau des Key Recovery Servers.

Key Recovery Server erbringen und wie sie miteinander kommunizieren. Eine solche zusammengehörende Menge in gleicher Weise zusammenarbeitender kommunizierender Key Recovery Server mit vergleichbaren Leistungsmerkmalen und gleichartigen Dienstleistungen (Form und Inhalt der archivierten Schlüssel, nutzbare Sicherheitsniveaus etc.) wird als Infrastruktur [16] oder auch Sicherungsinfrastruktur [18, 19] bezeichnet.

In einer Sicherungsinfrastruktur von Key Recovery Servern fallen u.a. die folgenden Aufgaben an:

- Gegenseitige Identifizierung und Authentifizierung der kooperierenden Key Recovery Server,
- Feststellung des Key Recovery Servers, dessen öffentlicher Schlüssel benutzt wurde,
- Bereitstellung des angeforderten Schlüssels für den kooperierenden Key Recovery Server,
- Strukturweite Identifizierung und Authentifizierung zum Retrieval berechtigter Endanwender.

Dazu erscheint ein spezieller, hochgradig abgesicherter Master Key Recovery Server angemessen, der die Aufgabe hat, die privaten Schlüssel der Key Recovery Server zu sichern und bei Bedarf wieder bereitzustellen. Wegen des Informationswerts der hier gespeicherten privaten Schlüssel sind Hochsicherheitsmaßnahmen angemessen wie sie etwa nach B1 (oder höher) TCSEC [35], den entsprechenden Stufen der IT-Security Evaluation Criteria [15] oder der Common Criteria [9] zertifizierte Systeme (Betriebssystem, Datenbanksystem, Kommunikationssystem, Anwendungssystem) mit zusätzlichen Maßnahmen der Kontrolle und Beobachtung [30] darstellen. Dieser Master Key Recovery Server kommuniziert ausschließlich mit den Key Recovery Servern.

In dieser Stufe entsteht bei der Speicherung der privaten Schlüssel in einem Master Key Recovery Server ein Overhead aus der Generierung mehrerer (hierarchischer) Key Recovery Felder. Es entsteht weiterhin Overhead bei der Speicherung und Übertragung der Key Recovery Felder: Der Speicherbedarf wird größer bzw. es müssen mehr Daten übertragen werden; letzteres kann bei schmalbandigen Kanälen zu grund-sätzlichen Problemen führen. Der insgesamt entstehende Overhead muß bei einem konkreten Produkt bewertet werden.

Zur Anpassung an unterschiedliche oder auch während der Lebensdauer des Key Recovery Servers steigende Sicherheitsforderungen muß das Sicherheitsniveau des Key Recovery Servers angemessen eingestellt werden können und die übrigen umgebungsabhängigen Sicherheitsmaßnahmen müssen angepaßt werden.

Von seiten des Unternehmens ist dazu in jedem Fall ein prüfbarer Vorgehensplan zu erstellen zusammen mit den zugehörigen Betriebs- und Sicherheitshandbüchern und es müssen die organisatorischen Abläufe und Geschäftsprozesse nachweisbar vertrauenswürdig definiert werden.

Es muß beim Unternehmen eine Überprüfung auf Einhaltung der Sicherheitsstrategie dergestalt vorgenommen werden, daß die Sender auf tatsächliche Hinterlegung der Schlüssel kontrolliert werden. Dies kann der Sicherheitsbeauftragten überprüfen, es kann auch durch gegenseitige Kontrolle der Key Recovery Felder durch Sender und Empfänger vorgenommen werden.

4. Auswahl- und Bewertungsparameter für Produkte

Entsprechend der Sicherheitsstrategie eines Unternehmens und den Ergebnissen der Risikoanalyse wird ein Sicherheitsniveau für die betrachtete Installation eines Key Recovery Servers festgelegt – z.B. entsprechend den beschriebenen Sicherheitsstufen. Anhand der dort geforderten Funktionen kann ein Produkt ausgewählt werden.

Beispielhaft werden im folgenden einige mögliche Auswahlparameter gegliedert aufgeführt, die über die allgemein zur Auswahl von Anwendungssoftware angewandten Kriterien (wie z.B. Hardware-/Software-Plattform) hinausgehen.

- Konstruktion des Key Recovery Produkts:
- Speichern, Retrieval von Schlüsseln, Zentrale – dezentrale Speicherung der Schlüssel, Vollständige - unvollständige Speicherung der Schlüssel.
- Performance:
  Durchsatz des Systems (Hardware/Software), Speicherbedarf je Schlüssel (inklusive Overhead), Anzahl möglicher Endanwender und Key Recovery Server, Speicherung (unterschiedlich) langer Schlüssel [4].
- Flexibilität:
  Unabhängigkeit von der Verfügbarkeit eines Key Recovery Servers beim Kommunikationspartner, Anschluß verschiedener Verschlüsselungsverfahren und -produkte, Anschluß verschiedener Key Management Protokolle, Interoperabilität mit verschiedenen Key Management Infrastrukturen – auch bei Einsatz unterschiedlicher Verschlüsselungsverfahren, Interoperabilität mit anderen Infrastrukturen.
- Sicherheitsniveau und Selbstschutz:
  Vertrauenswürdigkeit sicherheitsrelevanter Funktionen [15] entsprechend den zugrunde gelegten Sicherheitskriterien: Grundfunktionen, Widerstandswert der Mechanismen sowie Schwachstellen des Systems mit Betriebssystem, Kommunikationssystem, Datenbanksystem, Back-up, Archivfunktion. Sicherheitsrelevante Evaluierung: Black/crystal box. Vollständige Dokumentation und Quellcode, Konzelationsverfahren, Schlüssellänge, Skalierbarkeit des Sicherheitsniveaus (z.B. niedrig, Datenschutz, Gefahr für Leib & Leben), Umgehbarkeit des Gesamtsystems.
- Infrastruktur von Key Recovery Servern:
  Anzahl möglicher Key Recovery Server, Zentrale, dezentrale, verteilte Funktionen, Kooperation der Key Recovery Server: Gegenseitige Identifizierung/Authentifizierung, Datenaustausch, Identifizierung/Authentifizierung berechtigter Endanwender (Hinterlegung, Retrieval).
- Benutzerfreundlichkeit:
- Transparenz der Verfahren: Endanwender, Systemadministration, Antwortzeit: Archivierung, Retrieval.
- Aufwand:
  Auswahl und Betrieb des Verfahrens (Rechenzeit, Speicherkapazität, Bandbreite, Geräte, Administration), Kauf, Miete und Wartung des Produkts, Installation, Betrieb (Hinterlegung, Retrieval), Wartung, Pflege, Zertifizierung, Evaluierung, Akkreditierung, Sicherheitsüberprüfungen (Abnahme, Überprüfungen, Revision).
- Verfügbarkeit:
  Nationales Produkt: Zulassung/Erlaubnis für die (zivile) Nutzung – international uneingeschränkt. Ausländisches Produkt: Exportrestriktionen?

Kostenbetrachtung

Bei Alternativen von Key Recovery Produkten ist eine Kosten-/Nutzen-Betrachtung erforderlich um eine fundierte Auswahlentscheidung treffen zu können [26].

Untersuchungen zu den Kosten für unternehmensinterne Key Recovery Server liegen bisher nicht vor. Bewertet werden müßten bei einer Kostenbetrachtung – neben den Kosten für die Auswahlaktivitäten und die Beschaffung eines Produkts – insbesondere die folgenden Aspekte:

- Installation, Probebetrieb, Abnahme.
- Betrieb, Pflege und Wartung inklusive Einbindung in das Management der Informationsverarbeitung.
- Betreuung durch den Beauftragten für Informationssicherheit und die Revision.
- Schulung der Mitarbeiter.

Bekannt sind die Produkte der folgenden Unternehmen: SecureKeeS von CertCo [7, 50], SecureWays von IBM [22] und RecoverKey von TIS/NAI [66]. Die praxisorientierte Anwendbarkeit der dargestellten Konzepte, Sicherheitsstufen und Auswahlparameter wird im Fachbereich Angewandte Informatik der Fachhochschule Rhein-Sieg im Rahmen des Projekts SECFORS (Secure Electronic Commerce an der Fachhochschule Rhein-Sieg) produktbezogen überprüft.

Literatur

1. Abelson, H.; Anderson, R.; Bellovin, S. M.; Benahloh, J.; Blaze, M.; Diffie, W.; Gilmore, J.; Neumann, P. G.; Rivest, R. L.; Schiller, J. I.; Schneier, B.: The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption. . 1997 so auch Weck, G.: Key Recovery – Möglichkeiten und Risiken. Inf.- Spektrum 21, 3, S. 147 – 157 (1998) und Weck, G.: Key Recovery – Empfehlungen. Inf.- Spektrum 21, 3, S. 157 – 158 (1998)
2. Bellare, M.; Goldwasser, S.: Verifiable Partial Key Escrow. UCSD CSE Dept. Technical Report CS95–447. 1995
3. Blakley, G. R.: KRFeguarding Cryptographic Keys. Proc. of the National Computer Conference, American Federation of Information Processing Societies 48, 242 – 268, 1979
4. Blaze, M.; Diffie, W.; Rivest, R.; Shimomura, T.; Thompson, E.; Wiener, M.: Minimum Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security. . com/dist/mab/keylength.txt 1996
5. Caelli, W. J.; Longley, D.: Implementation of Key Escrow with Key Vectors to Minimise Potential Misuse of Key. National Computer Security Center – National Institute of Standards and Technolgy (Ed.): National Information Systems Security Conference Proceedings. Baltimore 1997
6. Cerny, D.; Pohl, H.: Trusted Third Parties und Sicherungsinfrastrukturen. Wirtschaftsinformatik 39, 6, 616 – 622 (1997)
7. CertCo – Bankers Trust Company: SecureKEES – The international passport for securing corporate information assets. 1995
8. Clark, A. J.: Key Recovery – Why, How, Who? Computers & Security 16, 8, 669 – 674 (1997)
9. Common Criteria Editorial Board (Ed.): Common Criteria for Information Technology Security Evaluation Version 2.0. 1998

10. Dam, K.; Lin, H. (Hrsg.):National Academy of Sciences: Cryptography's Role in Securing the Information Society. National Research Council. Washington 1996
11. Denning, D. E.: The Future of Cryptogryphy. 1996
12. Denning, D. E.: Descriptions of Key Escrow Systems. 1997
13. Denning, D. E.; Branstad, D. K.: A taxonomy for key escrow encryption systems. Communications of the ACM 30, 3, 34 – 40 (1996) und http://guru.georgetown.edu/~denning/crypto/taxonomy.html 1997
14. Denning, D. E.; Smid, M.: Key Escrow Today. IEEE Communications 32, 9, 58 – 68 (1994)
15. European Commission: Information Technology Security Evaluation Criteria (ITSEC). Provisional Harmonised Criteria. COM(90) 312. Brussels 1991
16. Geihs, K.: Infrastrukturen für heterogene verteilte Systeme. Inf.-Spektrum 16, 1, 11 – 23 (1993)
17. Gupta, S..: A Common Key Recovery Block Format: Promoting Interoperability Between Dissimilar Key Recovery Mechanisms. May 28, 1998
18. Hammer, V. (Hrsg.): Sicherungsinfrastrukturen – Gestaltungsvorschläge für Technik, Organisation und Recht. Heidelberg 1995
19. Hammer, V.: Gateway: Infrastruktur. Datenschutz und Datensicherung 22, 91 – 92 (1998)
20. Hewlett-Packard: International Cryptography Framework. 1996
21. Huhn, M.; Pfitzmann, A.: Technische Randbedingungen jeder Kryptoregulierung. In: Müller, G.; Pfitzmann, A. (Hrsg.): Mehrseitige Sicherheit in der Kommunikatiuonstechnik. Bonn 1997
22. IBM: Towards a framework-based solution to cryptographic key recovery http://www.ibm.com/security/html/ wp_keyrecarc.html. o.J.
23. ITU-T: Recommendation X.500 Series. ISO/IEC 9594, 1–9. Information Technology – Open Systems Interconnection: The Directory. (Previously: CCITT X.500 Recommendation)
24. ITU-T: Recommendation X.509 Open Systems Interconnection: The Directory: Authentication Framework. (Previously: CCITT X.509 Recommendation)
25. Key Recovery Alliance: Business Requirements for Key Recovery. Rel. 3.0 18, December 1997a
26. Key Recovery Alliance: Key Recovery and Electronic Commerce: Industry's Efforts to Develop New Tools to Support Strong Encryption. September 2, 1997b
27. Key Recovery Alliance: Public Policy Requirements for a Global Key Recovery Infrastructure. Sept. 2, 1997c
28. Krisis Consortium: An Analysis of Key Backup/Recovery Schemes. Project. 1998a
29. Krisis Consortium: The KRISIS Project. http://www.cordis.lu/infosec/src/study9.htm 1998b
30. Lessing, G.: Parameterspezifische Schwachstellenanalyse – Basisfunktionalität in geschotteteten Produktionsstätten. In: Bauknecht, K.; Büllesbach, A.; Pohl, H.; Teufel, S. (Hrsg.): .Sicherheit in Informationssystemen. Zürich 1998
31. Maher, D.P.: Crypto Backup and Key Escrow. Communications of the ACM 39, 3, 48 – 53 (1996)
32. Markham, T..: ISAKMP Key Recovery Extensions. June 5, 1998
33. Matyas, S. M.: Key Recovery Functional Model. June 8, 1998
34. Micali, S.: Fair Public-key Cryptosystem. Advances in Cryptology – CRYPTO 92'. Proceeding 113 – 138. Berlin 1993
35. National Computer Security Center: Trusted Computer System Evaluation Criteria. Fort Mead 1983
36. NIST (Hrsg.): Escrowed Encryption Standard. Federal Information Processing Standards Publication FIPS PUB 185. 1994
37. Oldehoeft, A.E. (Hrsg.): Report of the NIST Workshop on Key Escrow Encryption. NISTIR 5468 Gaithersburg 1994
38. Pohl, H.: Taschenlexikon: Sicherheit der Informationstechnik. Köln 1989
39. Pohl, H.: Entwicklung und Realisierung unternehmensübergreifender Sicherheitsarchitekturen. In: Hammer, K. et al. (Hrsg.): Synergie durch Netze. Magdeburg 1995
40. Pohl, H.: Guidelines for the Use of Names and Keys in a Global TTP Infrastructure. http://www. cordis.lu/infosec/ src/ ets.htm. Brussels 1997
41. Pohl, H.; Cerny, D.: Key Recovery Center. Arbeitsbericht. St. Augustin 1998a
42. Pohl, H.; Cerny, D.: Unternehmensinterne Schlüssel-Archive (Key Recovery Center). Wirtschaftsinformatik 40, 5, S. 443 – 446 (1998b)
43. Pohl, H.; Cerny, D.: Vertrauenswürdige Schlüsselarchive in Unternehmen. Ein Modell zur Skalierung von Sicherheitsmaßnahmen. In: Bischoff, R. et al. (Hrsg.): Von der Informationsflut zum Information Brokering. Braunschweig 1998c
44. Pohl, H.; Cerny, D.: Vertrauenswürdiger Einsatz von Enterprise Key Recovery Center – ein Modell zur Skalierung. In: Bodenbender et al. (Hrsg.): Management verteilter Systeme. Braunschweig 1999 – to be published. Vortrag auf der 13. Fachtagung des Fachauschusses 3.4 'Betrieb von Rechenzentren' der Gesellschaft für Informatik. 1999
45. Schneier, B.: Angewandte Kryptographie. Protokolle, Algorithmen und Source Code in C. Bonn 1996
46. Shamir, A.: How to share a secret. Communications of the ACM 22, 11, 612 – 613 (1979)
47. Shamir, A.: Partial Key Escrow: A New Approach to Software Key Escrow. In: NIST (Hrsg.): Key Escrow Standards Meeting. Gaithersburg 1995
48. Simmons, G.: An Introduction to Shared Secret and/or Shared Control Schemes and Their Applications. In: Simmons, G. (Ed.): Contemporary Cryptology: The Science of Information Integrity. 441 – 497, 1992
49. Stahlknecht, P.; Hasenkamp, U.: Einführung in die Wirtschaftsinformatik. Berlin 1997
50. Sudia, F. W.: Private Key Escrow System. New York 1995
51. Sweet, W. B.: Commercial Key Escrow (CKE): The Path to Global Information Security. Version 2.0. Glenwood 1996
52. Technology Committee of the Key Recovery Alliance: Cryptographic Information Recovery Using Key Recovery. Vers. 1.2 August 18, 1997
53. Technical Advisory Committee: Key Recovery Standard.. Advisory Committee Draft for an Federal Information Processing Standards Publication (FIPS PUBS). http://csrc.nist.gov/tacdfipsfkmi/FIPS698_ Word97.doc May 29, 1998
54. TIS – Trusted Information Systems: Exportable Strong Encryption: RecoverKey‰ CSPs. Glenwood 1996a
55. TIS – Trusted Information Systems: Worldwide Survey of Cryptographic Products. Glenwood 1996b
56. TIS – Trusted Information Systems: Key Recovery Centers: Key to Unlocking Key recovery. Glenwood 1996c
57. TIS – Trusted Information Systems: Task Title: Policy-Based Cryptographic Key Release System. Cryptographic Key Release Language Design and Specification. Glenwood 1996d
58. TIS – Trusted Information Systems: The RecoverKey‰ Toolkit: Your Key to Global Business. Glenwood 1996e

59. TIS – Trusted Information Systems (Walker, S.T.): TIS Recover-Key‰ – User-Controlled, Flexible Key Recovery. Glenwood 1997a
60. TIS – Trusted Information Systems (Walker, S.T.): Global Deployment and Use of Encryption. Glenwood 1997b
61. TIS – Trusted Information Systems: Principles for Use of Encryption and Key Recovery. Glenwood 1997c
62. TIS – Trusted Information Systems: TIS RecoverKey. Key Recovery Center V1.0. Glenwood 1998
63. Tompa, M.; Woll, H.: How to share a secret with Cheaters. Journal of Cryptology 1, 133 – 138 (1989)
64. Verheul, E.; Koops, B.-J.; Tilborg, H. v.: Binding Cryptography. A fraud-detectible alternative to key-escrow proposals. The Computer Law & Security Report 3 – 14, 1–2 (1997)
65. Walker, S. T.: A possible Basis for Software Key Escrow Encryption. In: Oldehoeft, A.E. (Hrsg.): Report of the NIST Workshop on Key Escrow Encryption. NISTIR 5468 Gaithersburg 1994
66. Walker, S. T.; Lipner, S. B.; Ellison, C. M.; Balenson, D. M.: Commercial Key Recovery. Communications of the ACM 39, 3, 41 – 47 (1996)
67. Wicke G., Huhn, M., Pfitzmann, A., Stahlknecht, P.: WI-Schlagwort Kryptoregulierung, Wirtschaftinformatik 39, 3, 279 – 282 (1997)
68. Williams, C.; Markham, T.: Key Recovery Header for IPSEC. April 8, 1998

Prof. Dr. Hartmut Pohl studierte Mathematik, Physik sowie Wirtschaftsinformatik und promovierte an der Universität Köln.
Er war an den Fachhochschulen Bochum und Gelsenkirchen tätig und vertritt seit 1997 das Fach Informationssicherheit im Fachbereich Angewandte Informatik der Fachhochschule Rhein-Sieg, St. Augustin.

Dietrich Cerny studierte Fernmelde-, Funk- und Radartechnik an der Höheren Technischen Schule der Luftwaffe in Neubiberg mit dem Abschluß als Dipl.-Ing.(FH). DV-Ausbildung in den USA. Ab 1967 Tätigkeit in der Planung und Realisierung des Führungsinformationssystems der Luftwaffe. Von 1990 bis zur Versetzung in den Ruhestand im Jahr 1996 Tätigkeit als Referent im Referat Sicherheit in der Informationstechnik im Bundesministerium des Innern.

Informatik
Forschung und Entwicklung

(Zusammenfassungen aktueller Veröffentlichungen in der Schwesterzeitschrift „Informatik Forschung und Entwicklung" Band 14, Heft 1, 1999)

Aufbereitung medizinischer Bilddaten

D. Zerfowski et al.

Es werden Verfahren zur Kompensation von Bewegungs- und Metallartefakten in tomographischen Aufnahmen vorgestellt, sowie neue Methoden der modellbasierten Registrierung von Datensätzen unterschiedlicher Modalitäten präsentiert.

Interaktive Visualisierung und Simulation zur Planung chirurgischer Eingriffe

H. Evers et al.

Der Artikel beschreibt aktuelle Ansätze zur Visualisierung und weiteren Bearbeitung medizinischer Volumendaten. Die Methodik verfolgt das Ziel, die präoperative Planung chirurgischer Eingriffe zu unterstützen, in dem Volumendaten interaktiv visualisiert und Gewebe wie auch funktionelle Einheiten simuliert werden.

Neue klinische Anwendungen der dreidimensionalen Rekonstruktion in der echographischen Diagnostik

G. Glombitza et al.

Dargestellt werden ein Beispiel aus der 3D-Echographie (Diagnose von Knochentumoren und ihren Auswirkungen auf das umgebende Weichgewebe) und zwei Beispiele aus der Echokardiographie (Vermessung von Herzklappenringen und Diagnose von Herzklappeninsuffizienzen durch Volumetrie und Visualisierung).

Ein Robotersystem für craniomaxillofaciale chirurgische Eingriffe

J. Raczkowsky et al.

Die Datenakquisition und Planung eines chirurgischen Eingriffs muß individuell für einen Patienten ausgeführt werden. Die präoperative Planung einer Operation auf den komplexen Freiformflächen des Patienten ist nur mit der Unterstützung eines rechnerbasierten Planungssystems durchführbar. Durch eine integrierte intraoperative Instrumentennavigation wird sichergestellt, daß die geplanten Vorgänge auch geometrisch richtig ausgeführt werden.

Text-Retrieval mit einem relationalen Datenbank-Management-System
Eine vergleichende Untersuchung

J. Kalinski

Es werden drei Realisierungen mittels SQL miteinander verglichen, von denen der Nested Loops Join mit vorsortierter Wortfolge am besten abschneidet. Dessen Effizienz beruht auf den signifikant unterschiedlichen Vorkommenshäufigkeiten der Anfragewörter.