(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 698 24 975 T2** 2005.08.25

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 097 553 B1**
(21) Deutsches Aktenzeichen: **698 24 975.5**
(86) PCT-Aktenzeichen: **PCT/IB98/01855**
(96) Europäisches Aktenzeichen: **98 952 968.0**
(87) PCT-Veröffentlichungs-Nr.: **WO 00/03525**
(86) PCT-Anmeldetag: **23.11.1998**
(87) Veröffentlichungstag der PCT-Anmeldung: **20.01.2000**
(97) Erstveröffentlichung durch das EPA: **09.05.2001**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **07.07.2004**
(47) Veröffentlichungstag im Patentblatt: **25.08.2005**

(51) Int Cl.[7]: **H04L 29/06**

(30) Unionspriorität:
98112938 13.07.1998 EP

(84) Benannte Vertragsstaaten:
AT, BE, CH, DE, ES, FR, GB, IE, IT, LI, NL, SE

(73) Patentinhaber:
International Business Machines Corp., Armonk, N.Y., US

(72) Erfinder:
HILD, G., Stefan, CH-8134 Adliswil, CH;
O'CONNOR, J., Luke, CH-8134 Adliswil, CH

(74) Vertreter:
Teufel, F., Dipl.-Phys., Pat.-Anw., 70569 Stuttgart

(54) Bezeichnung: **VERFAHREN ZUR ÜBERTRAGUNG VON INFORMATIONSDATEN VON EINEM SENDER ZU EINEM EMPFÄNGER ÜBER EINEN TRANSCODER**

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zur Übertragung von Daten von einem Sender über einen Transcoder (Codeumsetzer) zu einem Empfänger, wobei die Informationsdaten vor der Übertragung zum Empfänger verändert und/oder reduziert werden. Ferner betrifft die Erfindung ein Verfahren zur Codeumsetzung der Informationsdaten, insbesondere wenn diese verschlüsselte vertrauliche Informationsdaten sowie nicht-vertrauliche Informationsdaten umfassen. Die Erfindung betrifft auch ein Verfahren zum Empfangen der umgesetzten Informationsdaten in einem Empfänger und insbesondere die Prüfung der Integrität der Informationsdaten und der Sicherheit des Transcoders. Außerdem betrifft die Erfindung einen Sender, einen Transcoder und einen Empfänger, welche gemeinsam mittels der Transcoder-Funktionalität Informationsdaten übertragen können.

TECHNISCHES GEBIET UND HINTERGRUND DER ERFINDUNG

[0002] Gegenwärtig ist die Suche im Internet über das World Wide Web im Großen und Ganzen auf stationäre Benutzer mit Zugriff auf Browser beschränkt, die in leistungsfähigen Computern wie zum Beispiel Workstations oder PCs laufen. Derartige Rechner sind nicht nur über hinreichend schnelle Datenanschlüsse mit großer Bandbreite mit dem Internet verbunden, sondern auch mit leistungsfähiger Software and Hardware zur Verarbeitung und Darbietung der empfangenen Multimediadaten ausgestattet. Diese Infrastruktur wird von Autoren ausgiebig genutzt, um immer komplexere Webseiten zu erstellen; das betrifft sowohl die Dateninhalte selbst, die eine große Vielfalt von Audio- und Grafikformaten beinhalten können, als auch ausführbare Inhalte wie zum Beispiel Applets für anspruchsvollere Funktionen wie Zahlungsfunktionen usw.

[0003] Die Benutzer verlassen sich immer mehr auf das Internet als vielseitige Informationsquelle und möchten unterwegs immer häufiger unter Verwendung von mobilen Telefonen oder kleinen und leichten Taschencomputern auf das Internet zugreifen. Wenn Benutzer auf die vorhandene Infrastruktur des World Wide Web zuzugreifen versuchen, stoßen sie jedoch auf Probleme: Die Verbindung mobiler Taschencomputer mit dem Internet erfolgt über eine außergewöhnlich langsame und instabile Datenverbindung. Dabei benötigen ineffizient formatierte Datenströme unzumutbar lange Downloadzeiten.

[0004] Diese tragbaren Geräte weisen im Vergleich zu PCs üblicherweise nur bescheidene Datenverarbeitungsmöglichkeiten auf, da die verfügbare Rechenleistung begrenzt und die zur Darstellung der abgerufenen Inhalte verwendete Hardware relativ einfach ist. Zum Beispiel kann ein sehr einfacher mobiler Taschencomputer nur in der Lage sein, Textformate darzustellen.

[0005] Die über das Internet durch die Server bereitgestellten Inhalte werden jedoch unter der Voraussetzung erstellt, dass sie in einem relativ leistungsfähigen Rechner verarbeitet und angezeigt werden. Der Server könnte die Inhalte in unterschiedlichen Formen darstellen, wobei jede Darstellungsform auf einen bestimmten Rechner wie zum Beispiel einen Pager, ein Mobiltelefon, einen Laptop-Rechner, einen hochauflösenden PC usw. zugeschnitten ist. Hierfür ist es jedoch erforderlich, dass die Autoren große Teile der vorhandenen Serverdaten manuell neu bearbeiten müssen. Außerdem wäre es nicht wünschenswert, von jeder einzelnen Seite verschiedene Kopien zu speichern.

[0006] Eine alternative Lösung für den Client besteht darin, den Dienst eines Transcoders in Anspruch zu nehmen. Die Funktion des Transcoders besteht darin, den von einem Server empfangenen Inhalt umzuformatieren, um bei der zur Verfügung stehenden eingeschränkten Bandbreite zwischen Server und Client die zum Client übertragene Datenmenge zu reduzieren und sicherzustellen, dass die übertragenen Daten mit den Anzeige- und Verarbeitungsmöglichkeiten des Client dargestellt werden können.

[0007] Deshalb muss der Transcoder Kenntnis von der Datenverbindung zum Client und von den Verarbeitungs-/Anzeigemöglichkeiten des Client haben.

[0008] Zu den normalen Tasks, die der Transcoder an den für den Client bestimmten Inhalten ausführen kann, gehört das Entfernen von Audio- oder Grafikinhalten, das Umwandeln von Grafikformaten in andere Grafikformate, das Komprimieren und Dekomprimieren oder die Umwandlung aus einer Markup-Sprache wie zum Beispiel HTML in andere Datendarstellungen, z. B. in Sprache.

[0009] Üblicherweise durchlaufen sämtliche vom Server zum Client gesendeten Daten den Transcoder. Um die Codeumsetzung ausführen zu können, muss der Transcoder unbeschränkten Zugriff auf alle Daten haben. Da hierzu auch sicherheitsrelevante Informationen gehören können, sollte es sich beim Transcoder um eine gesicherte Einheit handeln. In diesem Fall kann die Sicherheit durch Einrichten eines Sicherheitskanals wie beispielsweise unter Verwendung des Secure-Socket-Layer-Protokolls (SSL) zwischen dem Server und dem Transcoder sowie eines separaten Sicherheitskanals zwischen dem Transcoder und dem Client oder durch Einbauen des Transcoders in den Server oder in den Client und Verwendung des SSL-Protokolls zwischen beiden gewährleistet werden. Wenn der Transcoder nicht

gesichert ist, beschränkt sich die Codeumsetzung auf Inhalte mit geringer oder ohne Bedeutung.

[0010] Leider kann die Einbeziehung der Transcoder-Funktionalität in den Server oder in den Client bis auf wenige hochsicherheitsrelevante Anwendungen nicht akzeptiert werden, da hierfür die Software und normalerweise auch die Hardware des Servers aufgerüstet werden muss. Außerdem kommen in kurzen Abständen neue mobile Geräte heraus, mit denen die Transcoder Schritt halten müssen, was zu kurzen Zyklen für das Ersetzen der Software führen würde.

[0011] Externe Transcoder-Dienste können kommerziell durch einen Taschencomputerhersteller, einen Datennetzbetreiber oder einen Internet-Serviceprovider angeboten und in die vorhandenen Proxy-Server integriert werden, was eindeutig eine geeignetere und skalierbare Lösung wäre. Allerdings können von Dritten bereitgestellte Transcoder nur selten als sicher eingestuft werden. In diesem Fall muss die Sicherheit durch Endpunkt-zu-Endpunkt-Verschlüsselung zwischen Server und Client gewährleistet werden, was den Transcoder vor die unmögliche Aufgabe stellen würde, den verschlüsselten Datenstrom zu verarbeiten.

[0012] In Verbindung mit vorhandenen Endpunkt-zu-Endpunkt-Verschlüsselungsverfahren können keine der bekannten Transcoder eingesetzt werden, da sie den Zugriff auf den Normaltext des gesamten Datenstroms benötigen. Da ihre Eingriffe durch die Clients nicht verifiziert werden können, sind sie für sicherheitsrelevante Datenübertragungen noch weniger geeignet.

[0013] Ein Transcoder wird z. B. in US 5544266 beschrieben. In US 5729293 wird eine Vorrichtung zur Codeumsetzung von eine Bildfolge darstellenden codierten digitalen Signalen beschrieben, welche einen Decodierungskanal variabler Länge und einen anschließenden Codierungs- und Decodierungskanal variabler Länge umfasst. Zwischen diesen beiden Kanälen ist eine Vorhersage-Untereinheit in Kaskaden geschaltet, wobei diese dritte Untereinheit zwischen zwei Subtraktoren in Reihe geschaltet ist und einen Bildspeicher und einen Schaltkreis zur Bewegungskompensation für Verschiebungsvektoren umfasst, welche die Bewegung jedes Bildes darstellen. Es sind auch andere Implementierungen möglich, insbesondere eine skalierbare Implementierung, bei der die Vorhersage-Untereinheit mindestens zwei bzw. allgemeiner gesagt eine Vielzahl ähnlicher, in Kaskaden geschalteter Codierungs- und Decodierungskanäle umfasst, die derselben Anzahl von Bildqualitätniveaus entsprechen.

[0014] In US-A-5 497 396 wird eine mit einer Datenübertragungsinfrastruktur verbundene Datenübertragungseinheit beschrieben, welche ein erstes Datencodierungsformat verwendet, das sich von einem innerhalb der Infrastruktur verwendeten zweiten Format unterscheidet, wobei die Datenübertragungsinfrastruktur ferner mindestens einen Daten-Transcoder zum Umsetzen in dem ersten Format codierter Daten in gemäß dem zweiten Format codierte Daten und umgekehrt umfasst. In der Infrastruktur ist in der Nähe des Anschlusses jeder das erste Format verwendenden Einheit ein Transcoder bereitgestellt. Durch das Verfahren zur Datenübertragung zwischen mindestens zwei dieser Einheiten wird anhand des durch jede der Einheiten verwendeten Datenformats der zwischen ihnen zu übertragenden Daten festgelegt, ob es erforderlich ist, zur Übertragung der Daten einen Transcoder zu verwenden. Wenn dies der Fall ist, wird derjenige Transcoder aktiviert, welcher der das erste Format verwendenden Einheit am nächsten gelegen ist, sodass die Daten in eine gemäß dem in der Infrastruktur verwendeten zweiten Format codierte Form überführt und möglichst in der Nähe der das erste Format verwendenden Einheit vom ersten in das zweite Format oder umgekehrt umgesetzt werden.

[0015] In EP-A-0811939 wird ein Verfahren beschrieben, durch das einem mit einem Server verbundenen Client ein Dokument bereitgestellt wird. Der Server stellt dem Client eine Anzahl von Internetdiensten bereit, wobei er unter anderem für den Client auch als Caching-Proxy-Server für den Internetzugriff fungiert. Im Proxy-Server befindet sich eine permanente Dokumentdatenbank, in der verschiedene Attribute aller zuvor als Reaktion auf eine Anforderung seitens eines Client abgerufenen Dokumente gespeichert werden. Wenn als Reaktion auf eine Anforderung seitens des Client ein Internetdokument von einem fernen Server abgerufen wird, wird die Datenbank abgefragt, und der Server verwendet die über das angeforderte Dokument gespeicherten Daten zum Umsetzen des Dokumentcodes. Der Dokumentcode wird zu verschiedenen Zwecken umgesetzt, unter anderem zum Umgehen von Bugs oder Quirks im Dokument, zum Formatieren des Dokuments für die Anzeige in einem Fernsehapparat, zur Verbesserung der Übertragungsgeschwindigkeit des Dokuments und zur Verringerung der Latenzzeit. Zur Ausführung dieser Funktionen bedient sich der Transcoder der Dokumentdatenbank. Die Dokumentdatenbank wird auch zum beschleunigten Abrufen zuvor angeforderter Dokumente und Bilder und zur Verringerung der Latenzzeit beim Herunterladen von Bildern zum Client verwendet.

[0016] In US 5745701 wird ein System zum Verbinden lokaler Netze über ein öffentliches Netz beschrieben, in welchem solche mit einem lokalen Netz verbundene Einheiten wie zum Beispiel Microcomputer in der Lage sind, über einen Router (Leitwegrechner) mit dem öffentlichen Netz verbunden zu werden, um mit der einen oder den mehreren mit dem mindestens

einen anderen lokalen Netz verbundenen Einheiten wie zum Beispiel Microcomputern Daten auszutauschen, welche wiederum in der Lage sind, über einen Router mit dem öffentlichen Netz verbunden zu werden. Das System implementiert einen Zertifikatsaustauschmechanismus und die Softwareprozeduren zur aktiven Authentifizierung des in den Routern installierten „Aufruf-Antwort"-Typs (challenge-response) und gewährleistet so beim Einrichten der Datenübertragung zwischen den lokalen Netzen über das öffentliche Netz die Sicherheit. Das beschriebene Netz stellt einen typischen Anwendungsbereich für den Einsatz der Codeumsetzung dar.

AUFGABE UND VORTEILE DER ERFINDUNG

[0017] Eine Aufgabe der Erfindung nach Anspruch 1 besteht darin, ein Verfahren zur Datenübertragung von einem Sender über einen Transcoder zu einem Empfänger bereitzustellen, das die Verwendung eines nicht gesicherten Transcoders zur Codeumsetzung von Informationsdaten ermöglicht, welche dennoch sowohl verschlüsselte vertrauliche als auch nicht-vertrauliche Informationsdaten umfassen können.

[0018] Das Verfahren mit den Merkmalen nach Anspruch 1 weist den Vorteil auf, dass trotz der Übertragung vertraulicher Informationsdaten in verschlüsselter Form die Codeumsetzung durchgeführt werden kann, indem die nicht-vertraulichen Informationsdaten umgesetzt werden, und die verschlüsselten vertraulichen Informationsdaten umgesetzt werden können, indem sie entfernt werden. Es sind kein gesicherter Transcoder und keine zusätzliche Datenübertragungsverbindung zwischen dem Sender und dem Empfänger zur Übertragung von vertraulichen Informationsdaten erforderlich.

[0019] Wenn die teilweise verschlüsselten Informationsdaten von Hash-Informationen begleitet werden, welche die Inhaltsverifikation zumindest eines Teils der teilweise verschlüsselten Informationsdaten im Empfänger ermöglichen, wird hierdurch ein zusätzlicher Sicherheitsmechanismus realisiert und somit die erreichbare Übertragungssicherheit erhöht und die Möglichkeit des Datenmissbrauchs minimiert.

[0020] Es erweist sich als vorteilhaft, wenn die Informationsdaten vor der Verschlüsselung und der Übertragung in Informationsdatenstücke aufgeteilt werden, weil hierdurch die Informationsdaten und insbesondere deren Parameter präziser und differenzierter verarbeitet werden können. Bei einem dieser Parameter handelt es sich um die Sicherheit, ob ein Informationsdatenstück vertraulich oder nicht-vertraulich ist. Bei einem anderen Parameter handelt es sich um den Codeumsetzungstyp, der angibt, welche Besonderheiten bei der Codeumsetzung der betreffenden Informationsdaten zu beachten sind, z. B. ob man das Informationsdatenstück wie oben erwähnt komprimieren bzw. weglassen kann.

[0021] Der oben erläuterte Vorteil wird noch größer, wenn jedem Informationsdatenstück ein eigener Stück-Sicherheitsinformationsteil und Stück-Codeumsetzungstyp-Informationsteil zugewiesen werden, sodass die Informationsdatenstücke ihr eigenes Profil besitzen, welches im vorliegenden Fall zumindest aus den Sicherheits- und den Codeumsetzungstypinformationen besteht. Dann kann der Transcoder die Informationsdaten entsprechend dem jeweiligen Profil gesondert behandeln. Wechselseitige Abhängigkeiten zwischen den Informationsdatenstücken sind dann ausgeschlossen.

[0022] Wenn ein Informationsdatenstück vorzugsweise Teil nicht-vertraulicher Informationsdaten ist und ihm ein eigener Stück-Hash-Informationsteil zugewiesen wird, kann bezüglich der Sicherheit eine genauere Differenzierung erreicht werden. Da man beim Hashverfahren davon ausgeht, dass der Inhalt der betreffenden Informationsdaten nicht verändert werden darf, kann man nur eine ganz bestimmte Codeumsetzungsfunktionalität verwenden, also entweder keine Codeumsetzung oder Löschen. Daher erweist es sich als vorteilhaft, dass ein solches Hashverfahren nur auf solche Informationsdaten beschränkt ist, bei denen es wirklich erforderlich ist, eine möglichst hohe Codeumsetzungswirkung zu erzielen.

[0023] Die Stück-Sicherheitsinformationsteile und die Stück-Codeumsetzungstyp-Informationsteile können entsprechend einer Umsetzungsstrategie in Markierungen umgesetzt und diese wiederum anstelle der Stück-Sicherheitsinformationsteile und der Stück-Codeumsetzungstyp-Informationsteile selbst zum Transcoder übertragen werden, wobei dem Transcoder eine Strategieinformation als Interpretationshilfe für diese Markierungen zur Verfügung gestellt wird oder bereits zur Verfügung steht. Durch diese Prozedur wird die zu sendende Datenmenge verringert. Das ist besonders dann der Fall, wenn eine große Anzahl von Stück-Sicherheitsinformationsteilen und Stück-Codeumsetzungstyp-Informationsteilen übertragen werden muss, weil die Datenreduktion durch Verwendung der kürzeren Markierungen die durch die Strategieinformation gelieferten zusätzlichen Daten immer mehr überwiegt. Dieses Verfahren lässt sich mit einer kurzen Kennung wie zum Beispiel einem Akronym vergleichen, das anstelle einer ausführlich zu erklärenden Aktion steht. Die Strategieinformation gibt dann an, welche Bedeutung die Kennung oder das Akronym hat.

[0024] Die Markierungen können dann zu einem Sicherheits- und Codeumsetzungstyp-Informationspaket zusammengefasst werden, das durch eine Signatur zur Verifikation der Integrität der Dateninhalte im

Empfänger vervollständigt wird. Der Vorteil hiervon besteht darin, dass der Empfänger nachweisen kann, ob das Sicherheits- und Codeumsetzungstyp-Informationspaket verändert wurde. Wenn das Paket nicht verändert wurde, kann der Empfänger prüfen, ob die empfangenen Informationsdaten gemäß den Regeln im Sicherheits- und Codeumsetzungstyp-Informationspaket umgesetzt wurden. Wenn dies nicht der Fall ist, weiß der Empfänger, dass der Transcoder nicht korrekt gearbeitet hat und er den empfangenen Informationsdaten nicht vertrauen kann.

[0025] Eine Aufgabe der Erfindung nach Anspruch 8 besteht darin, ein Verfahren zur Codeumsetzung von teilweise verschlüsselten Informationsdaten gemäß dem gewünschten Sicherheitsgrad bereitzustellen, welches nur auf Inhalte mit nicht-vertraulichen Informationsdaten zugreift.

[0026] Dieses Verfahren mit den Merkmalen nach Anspruch 8 ermöglicht die Codeumsetzung der empfangenen Informationsdaten auf vorteilhafte Weise, ohne auf Sicherheit Rücksicht nehmen zu müssen. Deshalb bedient es sich der Sicherheitsinformationen und der Codeumsetzungstypinformationen, aus denen der Transcoder erkennt, wie die eintreffenden Informationsdaten zu bearbeiten sind, und zwar welche Informationsdaten verschlüsselt sind und welche unverschlüsselt sind und welche Codeumsetzungsstrategie anzuwenden ist.

[0027] Eine Aufgabe der Erfindung nach Anspruch 13 besteht darin, ein Verfahren zum Empfangen der umgesetzten Informationsdaten im Empfänger bereitzustellen, wobei geprüft werden kann, ob der Transcoder die Sicherheits- und Codeumsetzungsbedingungen erfüllt hat.

[0028] Das Verfahren mit den Merkmalen nach Anspruch 13 hat den Vorteil, dass die Sicherheitsprüfung des Transcoders sehr einfach ist und auf denselben Informationen beruht, die der Transcoder zur Codeumsetzung verwendet hat. Da die Sicherheits- und Codeumsetzungstypinformationen nicht mit den Informationsdaten vermengt sind, wird eine Integritätsprüfung der Sicherheits- und Codeumsetzungstypinformationen erleichtert, da kein Ümsetzungs- und somit Änderungszugriff auf die Sicherheits- und Codeumsetzungstypinformationen erforderlich ist.

[0029] Die Verwendung von Markierungen als Kurzversion der Sicherheits- und Codeumsetzungstypinformationen ist besonders dann von Vorteil, wenn die hierfür eingesetzte Strategie, welche auch zum Interpretieren der Markierungen erforderlich ist, allgemein gebräuchlich und möglicherweise sogar standardisiert ist. Dann braucht die Strategieinformation nicht zusammen mit den Informationsdaten übertragen zu werden, da sie bereits im Transcoder vorliegt bzw. die Markierungen von diesem automatisch erkannt werden, weil die den Markierungen entsprechende Funktionalität bereits im Transcoder implementiert ist. Die Strategie kann dann im Transcoder direkt in die entsprechende Funktionalität integriert werden, sodass sich ein starrer Interpretationsschritt erübrigt. Wenn zum Beispiel eine Markierung „NT" ankommt, kann der Transcoder automatisch auf die Codeumsetzung verzichten, da er so programmiert oder eingestellt wurde, dass er bei Informationsdaten mit dieser Markierung keine Codeumsetzung durchführt. Die entsprechende Übersetzung würde dann lauten: „NT" = keine Codeumsetzung (no transcoding).

[0030] Das Paket der Sicherheits- und Codeumsetzungstypinformationen liefert dem Transcoder alle Informationen zur korrekten Verarbeitung der ankommenden Informationsdaten. Da die Sicherheits- und Codeumsetzungstypinformationen keiner Codeumsetzung unterzogen werden müssen, kann dieses Informationspaket mit einer Signatur versehen werden, anhand derer im Empfänger verifiziert werden kann, ob der Inhalt des Sicherheits- und Codeumsetzungstyp-Informationspakets irgendwo zwischen Sender und Empfänger verändert worden ist. Absichtliche oder zufällige Veränderungen des Sicherheits- und Codeumsetzungstyp-Informationspakets können dadurch im Empfänger leicht erkannt werden, wodurch die gesamte Informationsdatenübertragung sicherer wird.

[0031] Eine Aufgabe der Erfindung nach Anspruch 19 besteht darin, einen Sender zum Übertragen von Daten über einen Transcoder zu einem Empfänger bereitzustellen, bei dem man einen ungesicherten Transcoder zur Codeumsetzung von Informationsdaten verwenden kann, die dennoch sowohl verschlüsselte vertrauliche als auch nicht-vertrauliche Informationsdaten umfassen können.

[0032] Der Sender mit den Merkmalen nach Anspruch 19 hat den Vorteil, dass man die Vorteile der Codeumsetzung mit den Vorteilen der sicheren Übertragung von sicherheitsrelevanten, d. h. vertraulichen Informationsdaten vereinen kann, obwohl bei ihm im Vergleich zu bekannten Sendern nur einfache Änderungen erforderlich sind.

[0033] Teilungsmittel zum Aufteilen der Informationsdaten in Informationsdatenstücke vor dem Verschlüsseln und Übertragen lassen sich relativ leicht implementieren. Zum automatischen Ausführen des Teilungsprozesses kann man Textsyntax- oder Bilddaten-Headerinformationen verwenden.

[0034] Eine Aufgabe der Erfindung nach Anspruch 23 besteht darin, einen Transcoder zur Codeumsetzung von teilweise verschlüsselten Informationsdaten entsprechend der implizierten Sicherheit bereitzustellen, der mithin nur auf Inhalte mit nicht-vertraulichen Informationsdaten zugreift.

[0035] Der Transcoder mit den Merkmalen nach Anspruch 23 hat den Vorteil, dass er Informationsdaten mit verschlüsselten und unverschlüsselten Informationsdaten empfangen und insofern eine optimale Codeumsetzung durchführen kann, als er zur Codeumsetzung nur auf nicht-vertrauliche Informationsdaten zugreift, nicht aber auf verschlüsselte Informationsdaten. Je stärker sich der Transcoder mit den Informationsdaten vertraut machen kann, desto höher kann die Effizienz der Datenumsetzung sein, da er genauere Kenntnis darüber hat, welche Daten und wie weit diese reduziert werden können. Verschlüsselte Informationsdaten sind einer solchen Inhaltsanalyse jedoch nicht zugänglich, was durch den Sender auch beabsichtigt ist. Die erforderlichen Informationen darüber, welcher Teil der Informationsdaten wie zu behandeln ist, ist von den Sicherheits- und Codeumsetzungstypinformationen ableitbar.

[0036] Eine Aufgabe der Erfindung nach Anspruch 25 besteht darin, einen Empfänger zum Empfangen der umgesetzten Informationsdaten bereitzustellen, wobei geprüft werden kann, ob der Transcoder die Sicherheits- und Codeumsetzungsbedingungen eingehalten hat.

[0037] Der Empfänger mit den Merkmalen nach Anspruch 25 hat den Vorteil, dass er von dem Codeumsetzungsverfahren voll profitiert, ohne auf die Sicherheit des Transcoders angewiesen zu sein oder eine separate Übertragungsleitung für vertrauliche Daten zum Sender zu benötigen. Jegliche unerlaubten Veränderungen der Informationsdaten auf der Strecke zwischen dem Sender und dem Empfänger können anhand der Sicherheits- und Codeumsetzungstypinformationen leicht erkannt werden, welche selbst vor unerlaubten Veränderungen geschützt sind. Fälschungen der Informationsdaten können daher nicht unentdeckt bleiben bzw. werden mittels des Verschlüsselungsverfahrens vereitelt, was je nach dem verwendeten Verschlüsselungsalgorithmus einen sehr hohen Sicherheitsstandard bietet.

ÜBERBLICK ÜBER DIE ERFINDUNG

[0038] Das zu lösende Problem besteht darin, eine sichere Endpunkt-zu-Endpunkt-Übertragung zwischen einem Empfänger, wie z. B. einem Client, und einem Sender, wie z. B. einem Server, zu gewährleisten und dazwischen gleichzeitig eine Codeumsetzung zuzulassen, um die Inhalte entsprechend den Leistungsparametern und den Konnektivitätskenndaten des Client zu verändern. Die vorgeschlagene Lösung basiert auf dem Server, dessen Inhalte aus zwei Arten von Informationsdaten bestehen, und zwar solchen, die vertraulich sind und geschützt werden müssen, und solchen, die nicht-vertraulich oder sogar öffentlich sind und somit umgesetzt werden können. Dieser Ansatz verfolgt zwei Ziele:
Er ermöglicht die Anwendung von Codeumsetzungsverfahren auf einen sicherheitsrelevante Daten enthaltenden Datenstrom, wobei auf den unverschlüsselten Text der sicherheitsrelevanten Daten selbst nicht zugegriffen werden muss, und die durch den Transcoder erfolgte Codeumsetzung durch den Client verifizierbar ist.

[0039] Das Verfahren ermöglicht eine ungesicherte Codeumsetzung in einem sicherheitsrelevanten Datenstrom, ohne die Endpunkt-zu-Endpunkt-Verschlüsselung der im Datenstrom enthaltenen sicherheitsrelevanten Datenwerte zu beeinträchtigen.

[0040] Die Informationsdaten können in eine Gruppe von Feldern aufgeteilt werden, und zwar in vertrauliche und nicht-vertrauliche.

[0041] Außerdem ist das System insofern flexibel, als die Strategie zur Umsetzbarkeit des Codes und zur Sicherheit einzelner Datenfelder durch den Server festgelegt werden kann.

[0042] Außerdem können die durch den Transcoder durchgeführten Aktionen insoweit verifiziert werden, als der Transcoder nur Inhalte gemäß einer vorgegebenen Strategie verändert. Dabei geht man von der Voraussetzung aus, dass die Codeumsetzung der sicheren Felder der Inhalte nicht erforderlich ist.

[0043] Die Lösung kann auf Szenarien angewendet werden, bei denen E-Commerce, Online-Banking oder andere sicherheitsrelevante Anwendungen auf Clients der Stufe 0 oder Stufe 1 mit begrenzten Eingabe- oder Ausgabemöglichkeiten und Verbindungen mit begrenzter Bandbreite zu den Servern laufen, ohne dass in den Servern eine spezielle sichere Transcoder-Funktion installiert und verwaltet werden muss, oder bei denen eine schnelle Weiterentwicklung neuer und verbesserter Gerätefunktionen und somit auch Transcoder-Funktionen zu erwarten ist und deshalb eine unabhängige Codeumsetzung zu bevorzugen ist.

[0044] Ausgehend von einem ursprünglichen Informationsdatenstrom, der in Datenfelder aufgeteilt ist, die auch als Informationsdatenstücke bezeichnet werden, kann das hier vorgeschlagene Verfahren die folgenden Schritte umfassen:

– Einfügen zusätzlicher Kennungen bzw. Markierungen in den ursprünglichen Datenstrom, welche die Datenfelder bezüglich ihrer Umsetzungseigenschaften, z. B. umsetzbar, nicht umsetzbar, wahlweise, kritisch usw., und ihrer Sicherheitsrelevanz markieren, z. B. sicherheitsrelevant, nicht-sicherheitsrelevant usw., wobei diese Markierungen als Sicherheitsmarkierungen oder als Stück-Sicherheitsinformationsteil-Markierung und Stück-Codeumsetzungstyp-Informationsteil-Markierungen bezeichnet werden.
– Generieren eines Strategiedokuments, welches

für jede Kennung die für den Transcoder zugelassenen Operationen definiert. Dieses Strategiedokument oder die Strategieinformation liefert somit die Bedeutung der Markierungen, also wie diese zu verstehen sind. Dieser Schritt kann jedoch entfallen, wenn die Strategie dem Transcoder von vornherein bekannt ist.

– Separieren der sicherheitsrelevanten Informationsfelder und selektives und individuelles Anwenden der Endpunkt-zu-Endpunkt-Verschlüsselung auf diese Informationsfelder, sodass die nicht-sicherheitsrelevanten Informationsfelder unverschlüsselt bleiben.

– Generieren einer Dokumentübersicht, die auch als Sicherheits- und Codeumsetzungstyp-Informationspaket bezeichnet wird, auf Basis der Struktur des Originaldatenstroms, wobei die Übersicht die Sicherheitsmarkierungen und die Codeumsetzungstypmarkierungen enthält.

– Ermöglichen, dass der Empfänger, d. h. der Client, die Aktionen des Transcoders verifizieren kann, indem er die Ausgangsdaten des Transcoders mit der Dokumentübersicht und dem Strategiedokument vergleicht.

BESCHREIBUNG DER ZEICHNUNGEN

[0045] Beispiele der Erfindung sind in den Zeichnungen dargestellt und werden im folgenden anhand eines Beispiels ausführlich beschrieben. Die Erfindung ist in Fig. 1 mit einem Sender, einem Transcoder und einem Empfänger dargestellt.

[0046] Aus Gründen der Verständlichkeit zeigt die Figur weder die realen Abmessungen, noch befinden sich die Abmessungen zueinander im wirklichen Maßstab.

DETAILLIERTE BESCHREIBUNG DER ERFINDUNG

[0047] Im Folgenden werden verschiedene beispielhafte Ausführungsarten der Erfindung beschrieben.

[0048] In Fig. 1 ist ein als Server bezeichneter Sender **1** über eine Datenübertragungsverbindung, bei der es sich nicht unbedingt um eine physische Verbindung handeln muss, über einen Transcoder **2** mit einem Empfänger **3** verbunden. Dem Sender **1**, dem Transcoder **2** sowie dem Empfänger **3** steht eine Strategieinformation **17** zur Verfügung.

[0049] Der Sender **1** umfasst Teilungsmittel **21** zum Aufteilen der Informationsdaten **9** mit der Bezeichnung ID, die zum Empfänger **3** gesendet werden sollen. Am Ausgang der Teilungsmittel **21** liegen vertrauliche Informationsdaten **16** mit der Bezeichnung CD (confidential information data) und nicht-vertrauliche Informationsdaten **15** mit der Bezeichnung NCD (non-confidential information data) an. Zur Verschlüsselung der vertraulichen Informationsdaten **16** ist eine Verschlüsselungseinheit **5** angeordnet, welche die verschlüsselten vertraulichen Informationsdaten **14** mit der Bezeichnung ECD (encrypted confidential information data) liefert. Außerdem umfasst der Sender **1** eine Paketierungseinheit **23** und einen Signaturgenerator **22**.

[0050] Die hier als Informationsdaten bezeichneten Inhalte D können in eine Gruppe von N Inhaltsfeldern $f_1, f_2, ..., f_N$ zerlegt werden, die auch als Informationsdatenstücke bezeichnet werden. Ein Feld kann hier zum Beispiel einen Textabsatz, ein Bild oder formatierte Daten in einer Tabelle darstellen. Ferner kann es vorkommen, dass ein bestimmtes Feld f_i aus mehreren Teilfeldern $f_{i,1}, f_{i,2}, ..., f_{i,n}$ besteht, aus denen hervorgeht, dass die Inhalte hierarchisch geordnet sind. Zum Beispiel kann ein Absatzfeld f_i aus einem Textfeld, einem nachfolgenden Tabellenfeld, einem nachfolgenden Bildfeld und danach weiteren Textfeldern bestehen. Untergeordnete Felder können wiederum untergeordnete Felder enthalten usw. Die Feldstrukturierung obliegt dem Server. Die Aufteilung erfolgt durch Teilungsmittel **21**, welche die Felder auch nach ihrem gewünschten Sicherheitsgrad sortieren.

[0051] Wenn die Aufteilung in Felder abgeschlossen ist, weist der Server **1** jedem Feld f_i zwei Klassen von Markierungen zu bzw. fügt sie bei. Die erste Markierungsklasse L_s ist eine Sicherheitsmarkierung, die auch als Stück-Sicherheitsinformationsteil bezeichnet wird und anzeigt, ob dieses Feld f_i während der Übertragung verschlüsselt werden soll. Zum Beispiel kann der Satz möglicher Sicherheitsmarkierungen L_s (security labels) definiert werden zu

$$L_s = \{\text{sicher, unsicher}\} \quad (1)$$

und $L_s(f_i) \in L_s$, wobei $L_s(f_i)$ die Sicherheitsmarkierung von f_i ist. Die Markierung L_s kann auf verschiedene Weise erweitert werden, um beispielsweise den Verschlüsselungsgrad, z. B. mit kurzen oder langen Schlüsseln, oder Authentifizierungsinformationen oder eine Signatur zu beinhalten.

[0052] Die zweite Markierungsklasse L_t (transcoding labels) ist eine Codeumsetzungsmarkierung, die auch als Stück-Codeumsetzungstyp-Informationsteil bezeichnet wird und anzeigt, welche Aktion der Transcoder **2** ausführen kann, wenn ein Feld mit Inhalten empfangen wird. Ein möglicher Satz von Codeumsetzungsmarkierungen L_t kann zum Beispiel definiert werden zu

$$L_t = \{\text{nicht-umsetzbar, umsetzbar, kritisch, nicht-kritisch}\} \quad (2)$$

wobei die genaue Bedeutung dieser Markierungen in einer dem Server **1** zugehörigen Umsetzungsstrategie definiert wird. Eine solche Strategie kann zum

Beispiel darin bestehen, die Codeumsetzungsmarkierungen L_t wie folgt zu interpretieren:
‚umsetzbar' bedeutet, dass der Transcoder das Feld mit den Inhalten ohne Einschränkung umsetzen kann;
‚nicht-umsetzbar' bedeutet, dass der Transcoder **2** das vom Server **1** empfangene Feld mit den Inhalten nicht verändern darf;
‚kritisch' bedeutet, dass das Feld vom Transcoder **2** zum anfordernden Client **3** zu senden ist;
‚unkritisch' bedeutet, dass der Transcoder **2** das Feld aus den zum anfordernden Client **3** weitergeleiteten Inhalten löschen darf.

[0053] Der Server **1** kann eine Strategieanweisung pol(S) (policy statement), die den Satz von Sicherheits- und Codeumsetzungsmarkierungen $L_s(S)$ bzw. $L_t(S)$ enthält, sowie eine eindeutige Anweisung ausgeben, in der angegeben wird, wie die Markierungen zu interpretieren sind. Da die Strategieanweisung pol(S) keine sicherheitsrelevanten Daten enthält, kann sie jederzeit vom Server **1** abgerufen und zwischengespeichert werden, um sie später in einer Verbindung zum Server **1** zum Abrufen von Inhalten zu verwenden.

[0054] Im vorliegenden Fall wird davon ausgegangen, dass die Umsetzungsstrategie so gewählt wurde, dass sie den Regeln der dem Transcoder **2** bereits bekannten und verfügbaren Strategieinformation **17** folgt. Deshalb braucht hier keine Strategieanweisung pol(S) ausgegeben zu werden. Bei der bekannten Strategieinformation **17** kann es sich z. B. um eine üblicherweise verwendete Strategie, eine Art Standard handeln, der also vielen Transcodern, Sendern und Empfängern bekannt ist, sodass ein Sender die Strategieinformation **17** nicht erzeugen und absenden muss.

[0055] Der Inhalt D möge in die Felder f_1, f_2, ..., f_N, aufgeteilt worden sein und der Server **1** codiert dann jedes Feld f_i in einem Feldmarkierungstupel als

$$L(f_i) = <L_s(f_i), L_t(f_i), [H(f_i)]> \quad (3)$$

wobei $L_s(f_i)$ und $L_t(f_i)$ wie oben beschrieben definiert sind und H(...) eine auch als Hashinformationen oder als Hash bezeichnete kryptografische Hashfunktion wie zum Beispiel der Algorithmus SHA-1 ist. Die Hashfunktion $H(f_i)$, die auch auf kein, ein oder mehrere Felder f_i angewendet werden kann, wird auch als Stück-Hash-Informationsteil des Informationsdatenstücks bezeichnet und in eckigen Klammern als $[H(f_i)]$ angegeben, um sie als ein optionales Feld zu kennzeichnen. Ein Hash eines Feldes ist, wie später erläutert, in dessen Feldmarkierungstupel enthalten, wenn die Inhalte des Feldes durch den anfordernden Client **3** verifiziert werden sollen, wenn also die Felddaten unverschlüsselt und ohne Codeumsetzung gesendet werden.

[0056] Die Sicherheits- und Codeumsetzungsmarkierungen $L_s(f_i)$ und $L_t(f_i)$ können allgemein aus einer Liste der Werte von L_s und L_t bestehen. Zum Beispiel kann man bei Verwendung von L_t gemäß der Definition in (1) für ein Feld f_i eine Codeumsetzungsmarkierung

$$L_t(f_i) = \{\text{umsetzbar, unkritisch}\} \quad (4)$$

angeben, woraus hervorgeht, dass der Transcoder **2** die Wahl hat, ob eine Darstellung von f_i zum anfordernden Client gesendet werden soll, und ferner diese Darstellung auswählen kann. Bei einem Feld f_i mit den Teilfeldern $f_{i,1}$, $f_{i,2}$, ..., $f_{i,ni}$ wird das Codierungsschema in (2) rekursiv ausgeführt und liefert

$$L(f_i) = <L_s(f_i), L_t(f_i), L(f_{i,1}), L(f_{i,2}), ..., L(f_{i,ni}), [H(f_i)]> \quad (5)$$

und wenn $H(f_i)$ benötigt wird, wird es über das Feld und alle Teilfelder berechnet.

[0057] Die Markierung kann durch Markierungsmittel erfolgen, die mit den erforderlichen Informationen versorgt werden, damit sie wissen, welcher Teil der Informationsdaten **9** verschlüsselt werden soll und welcher Teil welcher Codeumsetzungsart unterworfen werden darf. Deshalb verwenden die Markierungsmittel die aus den Teilungsmitteln **21** kommenden Informationsdatenstücke als Eingangsdaten. Die Reihenfolge der Markierungen wird daher entsprechend der Reihenfolge der Informationsdatenstücke gewählt, um die Markierungen später, also im Transcoder **2** und im Empfänger **3**, den jeweiligen Informationsdatenstücken zuordnen zu können. Den Markierungsmitteln bzw. der Markierungseinheit können Benutzervorgaben zugeführt werden, damit diese weiß, welche Informationsdatenstücke zu verschlüsseln und/oder umzusetzen sind und wie dies erfolgen soll. Somit kann das Markieren nach einem automatischen System erfolgen, das die entsprechenden Markierungen automatisch zuweist, indem z. B. bestimmte vorgegebene Regeln und/oder bestimmte durch einen Benutzer eingegebene oder aus einer Liste abgeleitete Regeln oder individuelle Markierungsvorgaben befolgt werden. Mitunter kann das Markieren nach einem fest vorgegebenen Markierungsschema erfolgen und manchmal kann eine individuelle Markierungsliste die optimale Lösung darstellen, um der Markierungseinheit mitzuteilen, welcher Markierungswert welchem Informationsdatenstück zuzuweisen ist.

[0058] In der vorliegenden Beschreibung werden alle Sicherheitsmarkierungen unter der Bezeichnung SIL als Gruppe von Stück-Sicherheitsinformationsteilen bezeichnet, während die Gruppe der Codeumsetzungsmarkierungen unter der Bezeichnung TIL als Gruppe von Stück-Codeumsetzungstyp-Informationsteilen bezeichnet werden. Mit anderen Worten, jedes Feld bzw. jedes Informationsdatenstück hat ei-

nen eigenen Stück-Sicherheitsinformationsteil, wobei alle Stück-Sicherheitsinformationsteile die Sicherheitsinformationen bilden. Die Sicherheitsinformationen lassen sich in die Gruppe aller Sicherheitsmarkierungen und die zugehörigen Informationen der Codeumsetzungsstrategie unterteilen. Somit kann der Stück-Sicherheitsinformationsteil für jedes Feld in die Sicherheitsmarkierung und die entsprechende Codeumsetzungsstrategieinformation, kurz gesagt Strategieinformation, unterteilt werden.

[0059] Die TIL bildet zusammen mit der entsprechenden Strategieinformation die Codeumsetzungstypinformationen **13**, die in der Figur in vereinfachter Form dargestellt sind. Die SIL bildet zusammen mit der entsprechenden Strategieinformation die Sicherheitsinformationen **12**, die in der Figur ebenfalls in vereinfachter Form dargestellt ist. Das Prinzip besteht darin, dass der Transcoder **2** mit allen Informationen versorgt wird, die er zur Codeumsetzung gemäß den Vorgaben des Senders benötigt, die in einer dem Transcoder **2** verständlichen und zur korrekten Ausführung interpretierbaren Form ausgedrückt wird. Das bedeutet, dass die Sicherheitsinformationen **12** und die Codeumsetzungstypinformationen **13** in Form von Markierungen zum Transcoder **2** übertragen werden, der diese dann verstehen sollte, weil der Transcoder **2** bereits über die entsprechende Codeumsetzungsstrategie verfügt oder weil er die Markierungen aufgrund seiner Konstruktion direkt versteht oder weil ihm der Sender **1** oder eine andere Einrichtung die Strategieinformation **17** bereits mitgeteilt hat oder weil eine Markierungsstrategie entweder unerwünscht oder aus bestimmten Gründen nicht ausführbar ist und die nicht-markierten Sicherheitsinformationen **12** und die nicht-markierten Codeumsetzungstypinformationen **13** zum Transcoder **2** übertragen werden, sodass der Transcoder **2** zur direkten Ausführung der Codeumsetzung gemäß den empfangenen Sicherheitsinformationen **12** und Codeumsetzungstypinformationen **13** keine Strategieinformation benötigt.

[0060] Wenn das Markieren der Inhalte D abgeschlossen ist, kann der Server **1** die Inhalte D in der Form

$$Sum(D)=<L(f_1), L(f_2), ..., L(f_N)> \quad (6)$$

darstellen, was im Folgenden als Inhaltsübersicht von D bzw. als Sicherheits- und Codeumsetzungstyp-Informationspaket **11** mit der Bezeichnung sum(D) bezeichnet wird. Die Markierungen werden also durch eine Paketierungseinheit **23** in der Inhaltsübersicht sum(D) zusammengefügt. Dann signiert der Server **1** sum(D) und erhält sign(sum(D)), erzeugt also mittels des Signaturgenerators **22** eine Signatur **10**, die in der Figur mit SIG bezeichnet ist, um auf verifizierbare Weise eine Übersicht der Daten in den Inhalten D anzuzeigen. Nicht die Inhalte D selbst, sondern nur die Übersicht der Inhalte D sind signiert, da die eigentlichen Daten der einzelnen Felder in den Markierungsschemata in den Formeln (2) und (3) nicht enthalten sind. Die Inhaltsübersicht sum(D) ermöglicht es, die ein Inhaltsstück umfassenden Daten in kompakter Form darzustellen, was sich durch die Prüfung der Signatur sign(sum(D)) verifizieren lässt.

[0061] Die Funktionen der Paketierungseinheit und der Markierungseinheit können zu einer Funktion zusammengefasst werden.

[0062] Das Sicherheits- und Codeumsetzungstyp-Informationspaket **11** wird zum Transcoder **2** gesendet. Auch die verschlüsselten vertraulichen Informationsdaten **14** und die nicht-vertraulichen Informationsdaten **15** werden zum Transcoder **2** gesendet. Mit anderen Worten, die Informationsdaten **9** werden in aufgeteilter und teilweise verschlüsselter Form zum Transcoder **2** gesendet.

[0063] Um zu erläutern, wie eine sichere und verifizierbare Codeumsetzung erfolgt, soll ein Szenarium betrachtet werden, bei dem der Client **3** und der Server **1** eine sichere Sitzung für eine Endpunkt-zu-Endpunkt-Verschlüsselung mit dem Verschlüsselungsschlüssel K eingerichtet haben. Die vom Client **3** empfangenen Inhalte D sollen durch einen Codeumsetzungsdienst T gefiltert werden.

[0064] Für jede Einheit der angeforderten Inhalte D schlägt der Server **1** in der Inhaltsübersicht sum(D) nach und untersucht für jedes Feld f_i dessen in der Inhaltsübersicht sum(D) gefundenes Feldmarkierungstupel $L(f_i)$. Wenn die Inhalte D sicherheitsrelevante Daten enthalten, sind einige oder möglicherweise auch alle Felder mit einer Sicherheitsmarkierung ‚sicher' versehen.

[0065] Ohne den Anspruch auf Allgemeingültigkeit zu verlieren, wird angenommen, dass die ersten j Felder f_{1j}, f_{2j}, ..., f_j als gesichert und die übrigen Felder f_{j+1}, f_{j+2}, ..., f_N als ungesichert markiert sind. Dann sendet der Server **1** das folgende Tupel weiter zum Transcoder **2**:

$$<sum(D), sign(sum(D)), E_K(d(f_1)), ..., E_K(d(f_j)), d(f_{j+1}), ..., d(f_N)> \quad (7)$$

wobei $d(f_i)$ die zum Feld f_i gehörenden Daten und $E_K(d(f_i))$ die Verschlüsselung der zum Feld f_i gehörenden Daten mit dem Verschlüsselungsschlüssel K darstellen. Die Daten jedes gesicherten Feldes werden einzeln verschlüsselt.

[0066] Der Transcoder **2** umfasst mit TC gezeichnete Entscheidungsmittel **4** zum Entscheiden, welcher Teil der empfangenen teilweise verschlüsselten Informationsdaten **14**, **15** vor dem Senden zum Empfänger **3** umgesetzt werden soll.

[0067] Hierbei können die verschlüsselten vertraulichen Informationsdaten **14** nur ohne Verwendung ihrer Inhalte umgesetzt werden, während die nicht-vertraulichen Informationsdaten **15** unter Zugriff auf deren Inhalte umsetzbar sind.

[0068] Grundsätzlich ist unter der Codeumsetzung zu verstehen, dass der Umfang oder die Komplexität der empfangenen verschlüsselten vertraulichen Informationsdaten **14** verringert wird. Das kann unterschiedlich stark erfolgen, beispielsweise von einer sehr starken Codeumsetzung, die zu einer absoluten Minimalversion der verschlüsselten vertraulichen Informationsdaten **14** und der nicht-vertraulichen Informationsdaten **15** führt, bis hin zu einer ziemlich schwachen Codeumsetzung, bei der die verschlüsselten vertraulichen Informationsdaten **14** und die nicht-vertraulichen Informationsdaten **15** nur in geringem Maße reduziert werden. Die Codeumsetzung kann eine Datenkomprimierung oder eine teilweise Datenlöschung umfassen. Im vorliegenden Beispiel werden die Sicherheits- und Codeumsetzungstypinformationen **12**, **13** aus dem Sicherheits- und Codeumsetzungstyp-Informationspaket **11** gelesen und zur Codeumsetzung der verschlüsselten vertraulichen Informationsdaten **14** und der nicht-vertraulichen Informationsdaten **15** verwendet, was zu umgesetzten verschlüsselten vertraulichen Informationsdaten TECD **24** (transcoded encrypted confidential information data) und zu umgesetzten nicht-vertraulichen Informationsdaten TNCD **25** (transcoded non-confidential information data) führt.

[0069] Im vorliegenden Beispiel bearbeitet der Transcoder **2** den empfangenen Datenstrom **14**, **15** in zwei Schritten. Im ersten Schritt serialisiert der Transcoder die Daten durch Beseitigung der Teilfeldstruktur in jedem Feld. Wenn beispielsweise f_i ein Feld und $f_{i,j}$ ein Teilfeld von f_i ist, kann man sich die Serialisierung durch Ausführung der folgenden Operation vorstellen:

$$d(f_i)=<., d(f_{i,j}),.>---><.<ptr>,.>,ptr:<d(f_{i,j})>. \quad (8)$$

[0070] Die Serialisierung erfolgt dadurch, dass die Teilfelddaten durch einen Zeiger ersetzt werden, der auf die Stelle im Datenstrom zeigt, an der diese Daten zu finden sind. Das führt zu einer direkten, unverschachtelten Darstellung der hierarchischen Datenstruktur.

[0071] Im zweiten Schritt prüft der Transcoder **2** die nicht gesicherten Felder f_{j+1}, f_{j+2}, ..., f_N und führt eine geeignete Codeumsetzung durch, deren Ergebnis durch $T(f_{j+1}, f_{j+2}, ..., f_N)$ bezeichnet wird. Für jedes unkritische Feld f_i, das nach der Codeumsetzung aus dem abgehenden Datenstrom entfernt werden soll, prüft der Transcoder auch $d(f_i)$. Wenn $d(f_i)$ einen Zeiger auf Teilfelddaten enthält, werden auch diese Daten gelöscht. Wenn ein umsetzbares, zu entfernendes Feld ein gesichertes, verschlüsseltes Teilfeld enthält, wird $E_K(d(f_1))$, ..., $E_K(d(f_j))$ durch das Entfernen des Teilfeldes verändert, sodass $T(E_K(d(f_1))$,..., $E_K(d(f_j)))$ die Liste der verschlüsselten Felder anzeigt, die nach allen Löschungen infolge der Codeumsetzung übrig bleiben.

[0072] Zum Schluss sendet der Transcoder **2** das folgende 4-Tupel zum anfordernden Client **3** weiter:

$$<sum(D), sign(sum(D)), T(E_K(d(f_1)), ..., E_K(d(f_j))), T(d(f_{j+1}), ..., d(f_N))>. \quad (9)$$

[0073] Der Empfänger **3** umfasst Integritätsprüfmittel **6**, die die Signatur **10** überprüfen und als Integritätsprüfergebnis **19** eine Integritätsprüfinformation liefern, welche anzeigt, ob das Sicherheits- und Codeumsetzungstyp-Informationspaket **11** zwischen dem Sender **1** und dem Empfänger **3** bezüglich seines Inhalts verändert worden ist. Der Empfänger umfasst ferner einen Strategieinformationsinterpreter **8**, mit dessen Hilfe unter Verwendung der Strategieinformation **17** die Codeumsetzungstyp-Informationsmarkierungen **13** und die Sicherheitsinformationsmarkierungen **12** interpretiert werden können. Dieser Strategieinformationsinterpreter **8** ist nicht erforderlich, wenn der Empfänger bereits in der Lage ist, die Markierungssprache zu verstehen. Andererseits ist ein solcher Strategieinformationsinterpreter **8** im Transcoder **2** auch von Nutzen, wenn er die Markierungssprache nicht versteht, aber die Strategieinformation **17** nutzen kann.

[0074] Die interpretierten Markierungen dienen dann Vergleichsmitteln **7** zur Ermittlung, ob die umgesetzten verschlüsselten Informationsdaten **24** und die umgesetzten nicht-vertraulichen Informationsdaten **25** gemäß den in den Markierungen enthaltenen Regeln umgesetzt und behandelt worden sind. Als Ergebnis erhält man ein Anzeigeergebnis **27** zur Anzeige, ob die empfangenen Informationsdaten **24**, **25** mit umgesetztem Code gesichert sind. Zum Schluss werden die umgesetzten verschlüsselten Informationsdaten **24** durch eine Entschlüsselungseinheit **26** entschlüsselt, von der man als Entschlüsselungsergebnis **18** die decodierten vertraulichen Informationsdaten erhält. Die umgesetzten nicht-vertraulichen Informationsdaten **25** brauchen nicht weiter verarbeitet zu werden und werden direkt als umgesetzte nicht-vertrauliche Informationsdaten **20** ausgegeben.

[0075] Die Struktur der Originalinhalte D, wie sie im Server **1** vorlagen, wird durch sum(D) dargestellt und kann im Client **3** durch Prüfen der Serversignatur sign(sum(D)) in sum(D) verifiziert werden. Somit ist der Client **3** in der Lage, die Gruppe der D darstellenden Felder zu ermitteln, die der Server **1** angibt. Da das Sicherheits- und Codeumsetzungstyp-Informationspaket sum(D) die Markierungstupel für jedes Feld der Inhalte D enthält, kann der Client **3** ferner die

Markierungen verifizieren, die der Server **1** für die Felder der Inhalte D gewählt hatte. Insbesondere kann der Client **3** ermitteln, welche Felder durch den Server **1** als gesichert und welche durch den Server **1** als umsetzbar gekennzeichnet wurden.

[0076] Dann prüft der Client **3**, ob alle im Sicherheits- und Codeumsetzungstyp-Informationspaket sum(D) als gesichert und kritisch angegebenen Felder in den verschlüsselten Informationsdaten $T(E_K(Df_1)), ..., E_K(d(f_j)))$ durch den Transcoder **2** nicht gelöscht oder verändert worden sind. Im vorliegenden Beispiel erfolgt diese Verifikation zumindest zum Teil durch den Verschlüsselungsalgorithmus E, der Authentifizierungsinformationen über die verschlüsselten Daten enthalten kann.

[0077] Außerdem kann der Client **3** die Gruppe der in sum(D) angegebenen umsetzbaren Felder mit den empfangenen Feldern $T(d(f_{j+i}), ..., d(f_N)$ vergleichen, um zu verifizieren, dass der Codeumsetzungsprozess keinerlei Inhalte gelöscht oder unzulässig verändert hat, die im Client **3** dargestellt werden könnten.

Patentansprüche

1. Verfahren zur Übertragung von Informationsdaten (**9**) von einem Sender (**1**) über einen Transcoder (**2**) zu einem Empfänger (**3**), wobei die Informationsdaten (**9**) vertrauliche Informationsdaten (**16**) und nicht-vertrauliche Informationsdaten (**15**) umfassen,
dadurch gekennzeichnet, dass
die vertraulichen Informationsdaten (**16**) verschlüsselt werden, um verschlüsselte vertrauliche Informationsdaten (**14**) zu bilden, welche zusammen mit den nicht-vertraulichen Informationsdaten (**15**) teilverschlüsselte Informationsdaten (**14**, **15**) bilden,
und dass Sicherheitsinformationen (**12**) und Codeumsetzungstypinformationen (**13**) zusammen mit den teilverschlüsselten Informationsdaten (**14**, **15**) zum Transcoder (**2**) gesendet werden, wobei die Sicherheitsinformationen (**12**) und die Codeumsetzungstypinformationen (**13**) in einem Codeumsetzungsschritt vom Transcoder (**2**) verwendbar sind, durch den die verschlüsselten vertraulichen Informationsdaten (**14**) ohne Zugriff auf deren Inhalte umgesetzt werden, während die nicht-vertraulichen Informationsdaten (**15**) unter Zugriff auf deren Inhalte umgesetzt werden, wobei der Transcoder (**2**) beim Codeumsetzungsschritt entscheidet, welcher Teil der teilverschlüsselten Informationsdaten (**14**, **15**) zum Empfänger (**3**) übertragen und/oder vor der Übertragung verändert werden soll.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die teilverschlüsselten Informationsdaten (**14**, **15**) von Hash-Informationen begleitbar sind, durch welche der Inhalt mindestens eines Teils der teilverschlüsselten Informationsdaten (**14**, **15**) im Empfänger (**3**) verifiziert werden kann.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die Informationsdaten (**9**) vor der Verschlüsselung und der Übertragung in Informationsdatenstücke aufgeteilt werden.

4. Verfahren nach Anspruch 3, dadurch gekennzeichnet, dass jedem Informationsdatenstück ein eigener Stück-Sicherheitsinformationsteil und ein eigener Stück-Codeumsetzungstyp-Informationsteil zugewiesen wird.

5. Verfahren nach den Ansprüchen 1 bis 3 oder den Ansprüchen 1 bis 4, dadurch gekennzeichnet, dass mindestens einem der Informationsdatenstücke ein eigener Stück-Hash-Informationsteil zuweisbar ist, wobei das Informationsdatenstück vorzugsweise Teil der nicht-vertraulichen Informationsdaten (**15**) ist.

6. Verfahren nach Anspruch 4 oder nach den Ansprüchen 4 und 5, dadurch gekennzeichnet, dass die Stück-Sicherheitsinformationsteile und die Stück-Codeumsetzungstyp-Informationsteile gemäß einer Umsetzungsstrategie in Markierungen (SIL, TIL) umgesetzt werden, und dass anstelle der Stück-Sicherheitsinformationsteile und der Stück-Codeumsetzungstyp-Informationsteile die Markierungen (SIL, TIL) zum Transcoder (**2**) übertragen werden, wobei dem Transcoder (**2**) eine Strategieinformation (**17**) zur Verfügung gestellt wird oder bereits zur Verfügung steht, die erklärt, wie die Markierungen (SIL, TIL) zu interpretieren sind.

7. Verfahren nach Anspruch 6, dadurch gekennzeichnet, dass die Markierungen (SIL, TIL) zu einem Sicherheits- und Codeumsetzungstyp-Informationspaket (**11**) zusammengefasst werden, das durch eine Signatur (**10**) vervollständigt wird, welche im Empfänger (**3**) eine Integritätsverifikation der Inhalte erlaubt.

8. Verfahren zur Codeumsetzung von einem Sender (**1**) empfangener teilverschlüsselter Informationsdaten (**14**, **15**) in einem Transcoder (**2**), die zu einem Empfänger (**3**) übertragen werden sollen, wobei die teilverschlüsselten Informationsdaten (**14**, **15**) nicht-vertrauliche Informationsdaten (**15**) und verschlüsselte vertrauliche Informationsdaten (**14**) umfassen und von Sicherheitsinformationen (**12**) und Codeumsetzungstypinformationen (**13**) begleitet werden, wobei das Verfahren den Schritt des Entscheidens, welcher Teil der teilverschlüsselten Informationsdaten (**14**, **15**) vor der Übertragung zum Empfänger (**3**) umgesetzt werden soll, umfasst, wobei die verschlüsselten vertraulichen Informationsdaten (**14**) nur ohne Zugriff auf deren Inhalte umgesetzt werden können, während die nicht-vertraulichen Informationsdaten (**15**) unter Zugriff auf deren Inhalte umgesetzt werden können, und den Schritt der Codeumsetzung des Teils der teilverschlüsselten Informa-

tionsdaten (**14**, **15**) umfasst.

9. Verfahren nach Anspruch 8, dadurch gekennzeichnet, dass die teilverschlüsselten Informationsdaten (**14**, **15**) in der Form empfangen werden, dass sie in Informationsdatenstücke aufgeteilt sind.

10. Verfahren nach Anspruch 9, dadurch gekennzeichnet, dass jedem Informationsdatenstück ein eigener Stück-Sicherheitsinformationsteil und ein eigener Stück-Codeumsetzungstyp-Informationsteil zugeordnet ist.

11. Verfahren nach Anspruch 10, dadurch gekennzeichnet, dass die Stück-Sicherheitsinformationsteile und die Stück-Codeumsetzungstyp-Informationsteile in Form von Markierungen (SIL, TIL) empfangen werden, und dass zur Codeumsetzung eine dem Transcoder (**2**) zur Verfügung stehende Strategieinformation (**17**) verwendet wird, die erklärt, wie die Markierungen (SIL, TIL) zu interpretieren sind.

12. Verfahren nach Anspruch 11, dadurch gekennzeichnet, dass die Markierungen (SIL, TIL) zu einem Sicherheits- und Codeumsetzungstyp-Informationspaket (**11**) zusammengefasst empfangen werden, das durch eine Signatur (**10**) vervollständigt wird, welche im Empfänger (**3**) eine Integritätsverifikation der Inhalte erlaubt.

13. Verfahren zum Empfangen teilverschlüsselter Informationsdaten (**24**, **25**) mit umgesetztem Code von einem Transcoder (**2**) in einem Empfänger (**3**), welche nicht-vertrauliche Informationsdaten (**25**) mit umgesetztem Code und verschlüsselte vertrauliche Informationsdaten (**24**) mit umgesetztem Code umfassen, und ferner zum Empfangen von Sicherheitsinformationen (**12**) und Codeumsetzungstypinformationen (**13**) zusammen mit den teilverschlüsselten Informationsdaten (**24**, **25**) mit umgesetztem Code, wobei das Verfahren den Schritt des Vergleichens der Sicherheitsinformationen (**12**) und der Codeumsetzungstypinformationen (**13**) mit den teilverschlüsselten Informationsdaten (**24**, **25**) mit umgesetztem Code umfasst, um zu testen, ob die Codeumsetzung die Anforderungen der Sicherheitsinformationen (**12**) und der Codeumsetzungstypinformationen (**13**) erfüllt.

14. Verfahren nach Anspruch 13, dadurch gekennzeichnet, dass die teilverschlüsselten Informationsdaten (**14**, **15**) von Hash-Informationen begleitbar sind, durch welche der Inhalt mindestens eines Teils der teilverschlüsselten Informationsdaten (**24**, **25**) mit umgesetztem Code im Empfänger (**3**) verifiziert werden kann.

15. Verfahren nach Anspruch 13 oder 14, dadurch gekennzeichnet, dass die teilverschlüsselten Informationsdaten (**24**, **25**) mit umgesetztem Code in der Form empfangen werden, dass sie in Informationsdatenstücke aufgeteilt sind.

16. Verfahren nach den Ansprüchen 13 bis 15, dadurch gekennzeichnet, dass mindestens einem der Informationsdatenstücke ein eigener Stück-Hash-Informationsteil zugewiesen werden kann, wobei das Informationsdatenstück vorzugsweise Teil der nicht-vertraulichen Informationsdaten (**15**) ist.

17. Verfahren nach Anspruch 15 oder 16, dadurch gekennzeichnet, dass die Stück-Sicherheitsinformationsteile und die Stück-Codeumsetzungstyp-Informationsteile in Form von Markierungen (SIL, TIL) empfangen werden und dass der Empfänger (**3**) mittels einer ihm zur Verfügung stehenden Strategieinformation (**17**) die Markierungen (SIL, TIL) interpretiert und dadurch die korrekte Ausführung der Codeumsetzung testet.

18. Verfahren nach Anspruch 17, dadurch gekennzeichnet, dass die Integritätsverifikation der Inhalte eines die Markierungen (SIL, TIL) umfassenden Sicherheits- und Codeumsetzungstyp-Informationspakets (**11**) unter Verwendung einer Signatur (**10**) dieses Paketes erfolgt.

19. Sender (**1**) zum Übertragen von Informationsdaten (**9**) über einen Transcoder (**2**) zu einem Empfänger (**3**), wobei der Transcoder die Informationsdaten (**9**), welche vertrauliche Informationsdaten (**16**) und nicht-vertrauliche Informationsdaten (**15**) umfassen, vor der Übertragung zum Empfänger (**3**) umsetzt, dadurch gekennzeichnet, dass der Sender (**1**) eine Verschlüsselungseinheit (**5**) zum Verschlüsseln der vertraulichen Informationsdaten (**16**) umfasst und dass zusammen mit den teilverschlüsselten Informationsdaten (**14**, **15**) Sicherheitsinformationen (**12**) und Codeumsetzungstypinformationen (**13**) zum Transcoder (**2**) gesendet werden können, die der Transcoder (**2**) zur Codeumsetzung nutzen kann, wobei die verschlüsselten vertraulichen Informationsdaten (**14**) ohne Zugriff auf deren Inhalte umsetzbar sind, während die nicht-vertraulichen Informationsdaten (**15**) unter Zugriff auf deren Inhalte umsetzbar sind.

20. Sender (**1**) nach Anspruch 19, dadurch gekennzeichnet, dass dieser Teilungsmittel (**21**) zum Aufteilen der Informationsdaten (**9**) in Informationsdatenstücke vor der Verschlüsselung und der Übertragung umfasst.

21. Sender (**1**) nach Anspruch 20, dadurch gekennzeichnet, dass jedem Informationsdatenstück ein eigener Stück-Sicherheitsinformationsteil und ein eigener Stück-Codeumsetzungstyp-Informationsteil zugeordnet ist und dass anstelle der Stück-Sicherheitsinformationsteile und der Stück-Codeumset-

zungstyp-Informationsteile Markierungen (SIL, TIL) zum Transcoder (**2**) übertragbar sind, in welche die Stück-Sicherheitsinformationsteile und die Stück-Codeumsetzungstyp-Informationsteile gemäß einer Umsetzungsstrategie umsetzbar sind, wobei dem Transcoder (**2**) eine Strategieinformation (**17**) zur Verfügung gestellt wird oder bereits zur Verfügung steht, die erklärt, wie die Markierungen (SIL, TIL) zu interpretieren sind.

22. Sender (**1**) nach Anspruch 21, dadurch gekennzeichnet, dass er eine Paketierungseinheit (**23**) zum Zusammenfassen der Markierungen (SIL, TIL) zu einem Sicherheits- und Codeumsetzungstyp-Informationspaket (**11**) und einen Signaturgenerator (**22**) zum Vervollständigen des Paketes (**11**) durch eine Signatur (**10**) umfasst, welche im Empfänger (**3**) eine Integritätsverifikation der Inhalte erlaubt.

23. Transcoder (**2**) zur Codeumsetzung von einem Sender (**1**) empfangener teilverschlüsselter Informationsdaten (**14**, **15**) und zum Übertragen der teilverschlüsselten Informationsdaten (**24**, **25**) mit umgesetztem Code zu einem Empfänger (**3**), wobei die teilverschlüsselten Informationsdaten (**14**, **15**) nicht-vertrauliche Informationsdaten (**15**) und verschlüsselte vertrauliche Informationsdaten (**14**) umfassen und von Sicherheitsinformationen (**12**) und Codeumsetzungstypinformationen (**13**) begleitet werden, wobei der Transcoder (**2**) Entscheidungsmittel (**4**) umfasst, mittels deren entschieden wird, welcher Teil der empfangenen teilverschlüsselten Informationsdaten (**14**, **15**) vor der Übertragung zum Empfänger (**3**) umgesetzt werden soll, wobei die verschlüsselten vertraulichen Informationsdaten (**14**) nur ohne Zugriff auf deren Inhalte umsetzbar sind, während die nicht-vertraulichen Informationsdaten (**15**) unter Zugriff auf deren Inhalte umsetzbar sind.

24. Transcoder (**2**) nach Anspruch 23, dadurch gekennzeichnet, dass die teilverschlüsselten Informationsdaten (**14**, **15**) in der Form empfangen werden, dass sie in Informationsdatenstücke aufgeteilt sind und dass jedem Informationsdatenstück ein eigener Stück-Sicherheitsinformationsteil und ein eigener Stück-Codeumsetzungstyp-Informationsteil zugewiesen ist, welche in Form von Markierungen (SIL, TIL) empfangen werden, und dass zur Codeumsetzung eine dem Transcoder (**2**) zur Verfügung stehende Strategieinformation (**17**) verwendet werden kann, die dem Transcoder (**2**) erklärt, wie die Markierungen (SIL, TIL) zu interpretieren sind.

25. Empfänger (**3**) zum Empfangen teilverschlüsselter Informationsdaten (**24**, **25**) mit umgesetztem Code von einem Sender (**1**) über einen Transcoder (**2**), wobei die teilverschlüsselten Informationsdaten (**24**, **25**) mit umgesetztem Code nicht-vertrauliche Informationsdaten (**15**) und verschlüsselte vertrauliche Informationsdaten (**14**) umfassen, und ferner zum Empfangen von Sicherheitsinformationen (**12**) und Codeumsetzungstypinformationen (**13**) zusammen mit den teilverschlüsselten Informationsdaten (**24**, **25**) mit umgesetztem Code, wobei der Empfänger (**3**) Vergleichsmittel (**7**) zum Vergleichen der Sicherheitsinformationen (**12**) und der Codeumsetzungstypinformationen (**13**) mit den teilverschlüsselten Informationsdaten (**24**, **25**) mit umgesetztem Code umfasst, um zu testen, ob die Codeumsetzung die Anforderungen der Sicherheitsinformationen (**12**) und der Codeumsetzungstypinformationen (**13**) erfüllt.

26. Empfänger (**3**) nach Anspruch 25, dadurch gekennzeichnet, dass die teilverschlüsselten Informationsdaten (**24**, **25**) mit umgesetztem Code in der Form empfangen werden, dass sie in Informationsdatenstücke aufgeteilt sind, dass die Stück-Sicherheitsinformationsteile und die Stück-Codeumsetzungstyp-Informationsteile in Form von Markierungen (SIL, TIL) empfangen werden, und dass diese Markierungen (SIL, TIL) durch die Vergleichsmittel (**7**) unter Verwendung einer dem Empfänger (**3**) zur Verfügung stehenden Strategieinformation (**17**) und eines Strategieinformationsumsetzers (**8**) interpretierbar sind, und so die korrekte Ausführung der Codeumsetzung prüfbar ist.

27. Empfänger (**3**) nach Anspruch 26, dadurch gekennzeichnet, dass eine Integritätsverifikation der Inhalte eines die Markierungen (SIL, TIL) umfassenden Sicherheits- und Codeumsetzungstyp-Informationspaketes (**11**) durch Integritätsprüfmittel (**6**) unter Verwendung einer Signatur (**10**) des Paketes (**11**) durchführbar ist.

Es folgt ein Blatt Zeichnungen

Anhängende Zeichnungen

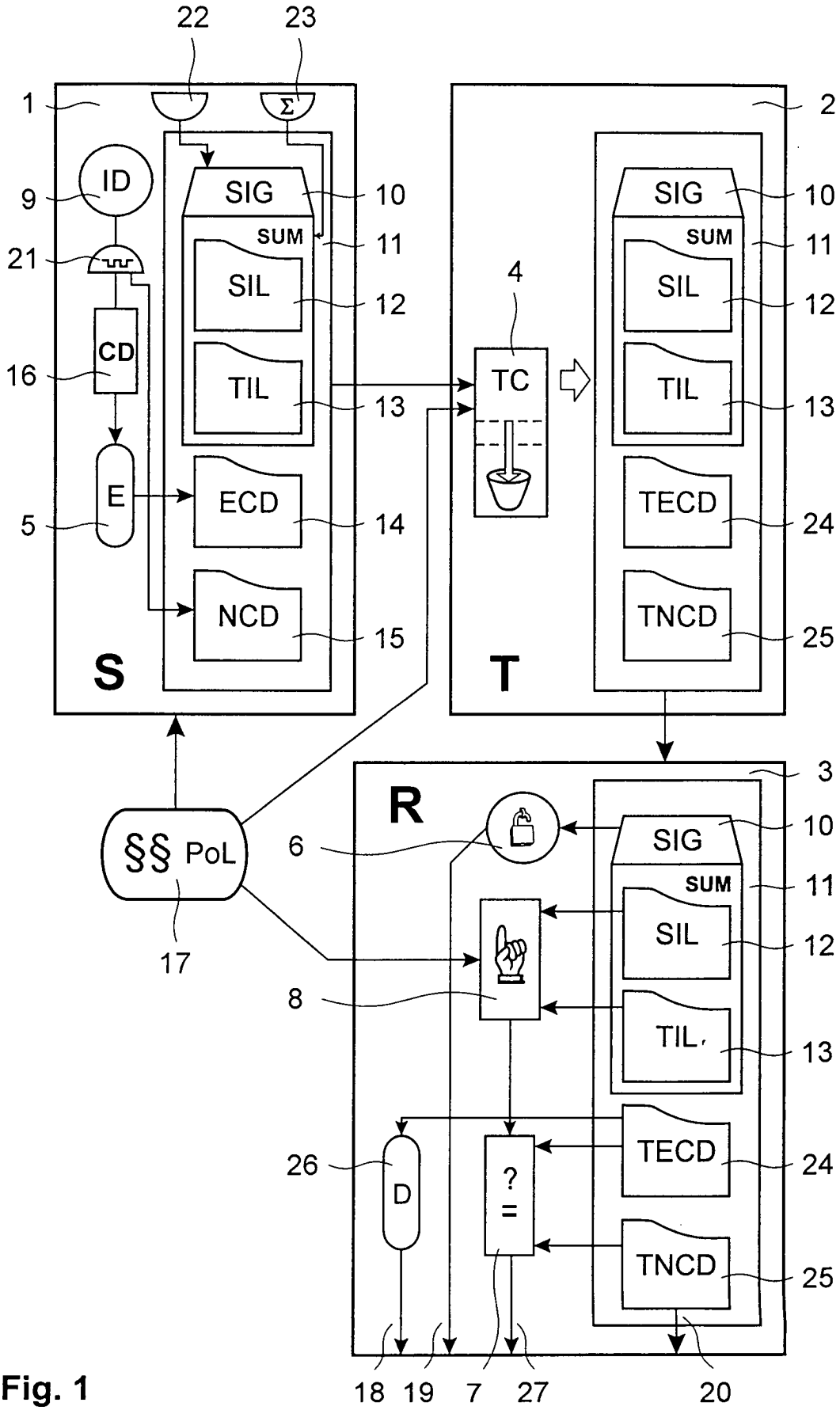

Fig. 1