(19) österreichisches patentamt

(10) **AT 503 291 A4 2007-09-15**

(12) Österreichische Patentanmeldung

(21) Anmeldenummer: **A 1928/2006**
(22) Anmeldetag: **21.11.2006**
(43) Veröffentlicht am: **15.09.2007**

(51) Int. Cl.[8]: ***G06F 12/14*** (2006.01),
G06Q 50/00 (2006.01)

(73) Patentanmelder:

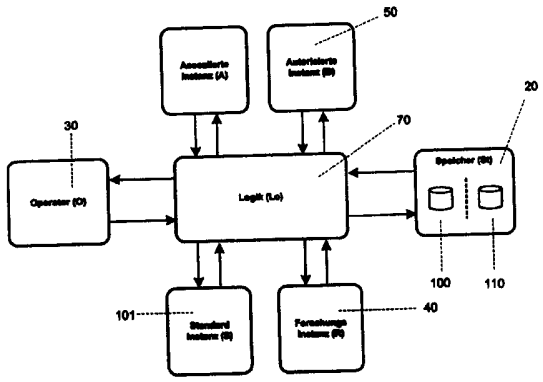
BRAINCON HANDELS-GMBH
A-1020 WIEN (AT)

(72) Erfinder:

RIEDL BERNHARD DIPL.ING. MAG.
HEIDENREICHSTEIN (AT)
NEUBAUER THOMAS DIPL.ING. MAG.
WIEN (AT)
BÖHM OSWALD ING.
WIEN (AT)

(54) DATENVERARBEITUNGSSYSTEM ZUR VERARBEITUNG VON OBJEKTDATEN

(57) Datenverarbeitungssystem zur Verarbeitung von Objektdaten einer Vielzahl von Standard-Instanzen (101), wobei Objektidentifikationsdaten (100) und Nutzdaten (110) in der Objektdaten-Datenbank (20) voneinander getrennt speicherbar und abrufbar sind, so dass allein aus den gespeicherten Datensätzen kein Zusammenhang zwischen den Objektidentifikationsdaten (100) und den Nutzdaten (110) ableitbar ist, wobei zumindest eine Eingabevorrichtung vorgesehen ist, welche bei Eingabe eines von für die Standard-Instanzen (101) vergebenen Sicherheitsschlüssel den Zugriff auf die Objektidentifikationsdaten (100) der zugeordneten Standard-Instanz und auf die zugehörigen Nutzdaten (110) ermöglicht, und der Sicherheitsschlüssel oder ein Teil davon bei der Standard-Instanz (101), bei der Wiedergewinnungsinstanz und gegebenenfalls bei weiteren von der Standard-Instanz bestimmten Instanzen (50, 60) verbleibt.



AT 503 291 A4 2007-09-15

ZUSAMMENFASSUNG

Datenverarbeitungssystem zur Verarbeitung von Objektdaten einer Vielzahl von Standard-Instanzen (101), wobei Objektidentifikationsdaten (100) und Nutzdaten (110) in der Objektdaten-Datenbank (20) voneinander getrennt speicherbar und abrufbar sind, sodaß allein aus den gespeicherten Datensätzen kein Zusammenhang zwischen den Objektidentifikationsdaten (100) und den Nutzdaten (110) ableitbar ist, wobei zumindest eine Eingabevorrichtung vorgesehen ist, welche bei Eingabe eines von für die Standard-Instanzen (101) vergebenen Sicherheitsschlüssel den Zugriff auf die Objektidentifikationsdaten (100) der zugeordneten Standard-Instanz und auf die zugehörigen Nutzdaten (110) ermöglicht, und der Sicherheitsschlüssel oder ein Teil davon bei der Standard-Instanz (101), bei der Wiedergewinnungs-Instanz und gegebenenfalls bei weiteren von der Standard-Instanz bestimmten Instanzen (50, 60) verbleibt.

(Fig.1)

Die Erfindung betrifft ein Datenverarbeitungssystem zur Verarbeitung von Objektdaten einer Vielzahl von Standard-Instanzen, wobei die Objektdaten Objektidentifikationsdaten und zugehörige Nutzdaten umfassen, mit einer Objektdaten-Datenbank, in welcher die Objektdaten über Zugriffseinrichtungen speicherbar und abrufbar sind.

Unter Standard-Instanz wird dabei eine Person, ein System od. dgl. verstanden, für die schützenswerte Objektdaten bestehen. Diese Objektdaten enthalten Objektidentifikationsdaten, die eine Identifizierung eines Objekts, z.B. über die Sozialversicherungsnummer einer Person, ermöglichen und Nutzdaten, die zu dem jeweiligen Objekt generiert wurden und gespeichert sind.

Da immer mehr Datenbanken, z.B. mit personenspezifischen Daten existieren oder im Entstehen sind, wird ein verstärkter Schutz von objektbezogenen, z.B. persönlichen Angaben und Daten angestrebt. Andererseits werden in vielen Bereichen, z.B. im Gesundheitsbereich Daten von Personen und zugehörige Meß- und Überwachungsdaten sowie historische Daten zu Studienzwecken und für statistische Analysen sowie für die Umsetzung von gesetzlichen Bestimmungen benötigt und daher über längere Zeit aufbewahrt, um sie einer späteren Verarbeitung zuzuführen. Dies führt zu einem verstärkten Schutzbedürfnis der gespeicherten Daten.

Es bestehen daher seit jeher Bestrebungen, einerseits die Vorteile der Verfügbarkeit von möglichst vielen Datensätzen nützen zu können, andererseits aber nicht die Privatsphäre zu verletzen. Aus diesen Gründen wird bei bestehenden Lösungsansätzen versucht, die Daten jeder einzelnen Person, die dem Datenschutz unterliegen, vor dem Zugriff von nichtautorisierten Benutzern zu bewahren.

Bestehende Systeme bieten jedoch keinen ausreichenden Schutz gegen eine Rückverfolgung von Daten durch Vergleich und unterbinden somit nicht die Möglichkeit, einen Rückschluss auf die Identität der Standardinstanz durch Vergleich der Nutzdaten, z.B. der Krankengeschichte eines Patienten, vorzunehmen.

Bei bestehenden Datenverarbeitungssystemen wird diese Zuordnung beispielsweise im System zentral durch einen Zugangskode geschützt bzw. erfolgt unter Verwendung einer Liste. Wer sich somit über diesen zentralen Zugangskode Zutritt zu den Daten verschaffen kann, dem stehen die Gesamtheit oder große Teile aller Datenbestände zur Verfügung. Dies bereitet nicht nur Probleme bei einem zentralen Hacker-Angriff auf das System, sondern wirft ganz generell die Frage auf, wer die Kontrolle über die Datenbestände im System hat und ob nicht die Gefahr der unautorisierten Datenweitergabe durch die Systemoperatoren eintreten kann.

Aufgabe der Erfindung ist es daher, ein Datenverarbeitungssystem der eingangs genannten Art zu schaffen, bei welchem erhöhte Sicherheit gegen Datenmissbrauch gegeben ist, dennoch aber bei Bedarf die Zuordnung von Personenidentifikationsdaten und Nutzdaten über längere Zeiträume möglich ist.

Weitere Aufgabe der Erfindung ist es, ein Datenverarbeitungssystem anzugeben, welches die Möglichkeit eines Zugriffes auf Nutzdaten eines Objekts ermöglicht, ohne die Objektidentifikationsdaten dieses Objekts preiszugeben.

Erfindungsgemäß wird dies dadurch erreicht,

- daß die Objektidentifikationsdaten und die Nutzdaten in der Objektdaten-Datenbank voneinander getrennt speicherbar und abrufbar sind, sodaß allein aus den gespeicherten Datensätzen kein Zusammenhang zwischen den Objektidentifikationsdaten und den Nutzdaten ableitbar ist,

- daß zumindest eine Eingabevorrichtung vorgesehen ist, welche bei Eingabe eines von für die Standard-Instanzen vergebenen Sicherheitsschlüssel den Zugriff auf die Objektidentifikationsdaten der zugeordneten Standard-Instanz und auf die zugehörigen Nutzdaten ermöglicht,

- daß gegebenenfalls für jede der Standard-Instanzen eine oder mehrere zugeordnete Wiedergewinnungs-Instanzen außerhalb der Objektdaten-Datenbank definiert sind, über welche bei Verlust des Sicherheitsschlüssels dieser wieder erzeugt werden kann, und

- daß der Sicherheitsschlüssel oder ein Teil davon bei der Standard-Instanz verbleibt und gegebenenfalls zusätzlich bei der Wiedergewinnungs-Instanz und/oder bei weiteren von der Standard-Instanz bestimmten Instanzen verbleibt oder von diesen auf ihn zugegriffen werden kann.

Der Sicherheitsschlüssel kann aus verschiedenen Teilschlüsseln zusammengesetzt und in sich verschlüsselt sein. Ein Teil-Sicherheitsschlüssel kann dabei einen anderen Teil-Sicherheitsschlüssel entschlüsseln, welcher seinerseits weiteren Instanzen oder der bzw. den Wiedergewinnungs-Instanzen zugänglich gemacht ist. Damit ist der Schutz der Daten gewährleistet und bei Verlust des Sicherheitsschlüssels kann die Berechtigung zum Datenzugriff für die Standard-Instanz wiederhergestellt werden.

Es sind somit zwei getrennte Datengruppen vorgesehen, nämlich die Objektidentifikationsdaten und die Nutzdaten, die den Standard-Instanzen zugeordnet sind. Letztere Nutzdaten einer bestimmten Standard-Instanz können mit den Objektidentifikationsdaten derselben nur in Verbindung gebracht werden, wenn der für die jeweilige Standard-Instanz vergebene Sicherheitsschlüssel zur Anwendung gebracht wird.

Auf diese Weise sind die Daten jeder Standard-Instanz durch einen individuellen Sicherheitsschlüssel geschützt, der vorzugsweise in Teilen dezentral bei der Standard-Instanz selbst und bei der bzw. den Wiedergewinnungs-Instanzen oder anderen Instanzen verbleibt und nicht zentral abgefragt werden kann bzw. nur unter Bekanntgabe eines Sicherheitsschlüssel. Im Falle eines Verlustes oder einer Zerstörung des Sicherheitsschlüssels durch die Standard-Instanz kann der Zugriff

auf die Objektdaten der Standard-Instanz z.B. über die Wiedergewinnungs-Instanzen geschehen.

Gemäß einer Ausführungsform der Erfindung können mehrere voneinander unabhängige Systemoperator-Instanzen vorhanden sein, aus denen zwei oder mehrere Systemoperator-Instanzen für jeweils eine der Standard-Instanzen als die dieser zugeordneten Wiedergewinnungs-Instanz definiert sind, ohne daß den ausgewählten Systemoperator-Instanzen die Identität der jeweils anderen ausgewählten Systemoperator-Instanz(en) sowie der Standard-Instanz(en) bekannt ist, wobei den zumindest zwei ausgewählten Systemoperator-Instanzen ein gemeinsamer Zugriff auf die Objektdaten und die zugehörigen Nutzdaten für die jeweilige Standard-Instanz möglich ist.

Die ausgewählten Systemoperator-Instanzen sind z.B. nach einem Zufallsprinzip so ausgewählt, daß sie voneinander unabhängig, vorzugsweise räumlich getrennt sind und nicht voneinander wissen, wer für welche Standard-Instanz einen der Teilschlüssel verwahrt, die gemeinsam mit dem oder den anderen Teilschlüsseln einen Zugriff auf die Objektdaten und Nutzdaten der zugeordneten Standard-Instanz erlauben, sodaß auf diese Weise ein neuer Sicherheitsschlüssel für die betroffene Standard-Instanz generiert und wieder vergeben werden kann.

Die Standard-Instanz ist jeweils Inhaberin ihrer Daten und hat die unbeschränkte Berechtigung anderen Instanzen diese Berechtigung zu verleihen. In weiterer Ausbildung der Erfindung können daher weitere Instanzen definiert sein, welche durch die Standard-Instanzen zum vollen oder teilweisen Datenzugriff autorisiert sind.

Weiters können gemäß einer Ausführungsform der Erfindung die weiteren Instanzen eine oder mehrere assoziierte Instanzen umfassen, die jeweils durch eine der Standard-Instanzen autorisiert sind und die gleiche Zugriffsberechtigung wie diese aufweisen sowie weitere Instanzen autorisieren können.

Eine solche assoziierte Instanz befindet sich in der Hierarchie unmittelbar unterhalb der Standard-Instanz, kann auf alle Daten der Standard-Instanz zugreifen und weiteren Instanzen ebenfalls diese Berechtigung ermöglichen.

Es kann auch vorgesehen sein, daß in einer weiteren Ausführungsform der Erfindung die weiteren Instanzen eine oder mehrere autorisierte Instanzen umfassen, die jeweils durch eine der Standard-Instanzen autorisiert sind, auf vorbestimmte Einträge in der Objektdaten-Datenbank zuzugreifen. Die autorisierte Instanz kann sowohl von der Standard-Instanz als auch von der assoziierten Instanz zum eingeschränkten Zugriff berechtigt werden.

Zum Zweck der Auswertung von Nutzdaten ohne Berechtigung zum Zugriff auf Objektidentifikationsdaten können die weiteren Instanzen eine oder mehrere Forschungs-Instanzen umfassen. Die Forschungs-Instanzen können daher nur Nutzdaten einsehen.

Um Einträge von Nutzdaten in der Objektdaten-Datenbank für eine bestimmte Standard-Instanz abrufen zu können, kann jedem Eintrag mit Nutzdaten in der Objektdaten-Datenbank eine eindeutige Nutzdaten-Identifikation zugeordnet sein.

Für die Aufbewahrung jenes Teils des Sicherheitsschlüssels einer bestimmten Standard-Instanz, der bei dieser verbleibt, bestehen verschiedenste Möglichkeiten.

Gemäß einer bevorzugten Ausführungsform der Erfindung kann der Sicherheitsschlüssel oder Teile davon auf einem Sicherheitstoken gespeichert sein, z.B. auf einer Smartcard, welche über einen PIN-Kode verfügt. Damit kann auch ein langer Sicherheitsschlüssel für den Anwender bequem eingegeben werden. Die Standard-Instanz meldet sich dabei über das Einziehen der Smartcard und Eingeben des PIN-Kodes im jeweiligen System an und kann auf diese Weise den auf der Smartcard gespeicherten Sicherheitsschlüssel bekanntgeben.

Der Sicherheitsschlüssel verbleibt bei der Standard-Instanz und ist nicht zentral einsehbar.

In weiterer Ausbildung der Erfindung kann die Objektdaten-Datenbank durch zwei separate Datenbanken gebildet sein, wobei in der einen Datenbank Objektidentifikationsdaten und in der anderen Datenbank Nutzdaten gespeichert sind. Durch die diese räumliche Trennung der Datensätze des erfindungsgemäßen System wird eine erhöhte Sicherheit erreicht.

Das Anwendungsgebiet der Erfindung ist hinsichtlich der Art der Objektdaten in keiner Weise eingeschränkt. Eine mögliche Anwendung besteht aber darin, daß die Objektdaten-Datenbank eine Personendaten-Datenbank ist und die Objektidentifikationsdaten Personendaten, insbesondere Patientendaten sind.

Wie bereits erwähnt, kann der Sicherheitsschlüssel zwei- oder mehrteilig ausgebildet sein, sodaß ein äußerer Schlüssel bei der Standard-Instanz verbleibt und über diesen auf einen nächstinneren Schlüssel zugegriffen bzw. dieser durch Entschlüsselung zugänglich gemacht werden kann. Dieser nächstinnere Schlüssel kann wiederum auf den seinerseits nächstinneren Schlüssel zugreifen, usw. Dies hat den Vorteil, daß bei Verlust des äußeren Schlüssels durch die Standard-Instanz eine weitere Instanz berechtigt sein kann, auf den nächstinneren Schlüssel zuzugreifen bzw. diesen durch Entschlüsselung zugänglich zu machen. Der Datenzugriff wird durch Entschlüsselung bis zur innersten Schale oder Schicht ermöglicht, wonach wieder ein neuer äußerer Schlüssel gebildet werden kann, welcher der betroffenen Instanz zur Verfügung gestellt wird.

Eine Ausführungsform der Erfindung kann darin bestehen, daß der Sicherheitsschlüssel jeder der Standard-Instanzen aus einem inneren und einem äußeren Schlüssel sowie einem Schlüssel für den jeweiligen Nutzdaten-Datensatz gebildet ist, wobei die Nutzdaten und die Objektidentifikationsdaten der jeweiligen Standard-Instanz optional mit dem inneren Schlüssel verschlüsselt sind, wobei der äußere Schlüssel jeweils bei den Standard-Instanzen, der innere Schlüssel bei den

Wiedergewinnungs-Instanzen und gegebenenfalls den assoziierten Instanzen verbleibt und der innere Schlüssel mit dem zugehörigen äußeren Schlüssel, sowie der innerste Schlüssel für den jeweiligen Nutzdaten-Datensatz mit dem inneren Schlüssel verschlüsselt ist. Die jeweiligen Schlüssel können für alle Instanzen gleich oder aber auch verschieden gewählt werden.

Die Erfindung betrifft weiters ein Verfahren zur Verarbeitung von Objektdaten von Standard-Instanzen, welche Objektidentifikationsdaten und zugehörige Nutzdaten umfassen, wobei in einem Speicherschritt die Objektdaten in einer Objektdaten-Datenbank gespeichert und in einem Abfrageschritt aus der Objektdaten-Datenbank auf die Objektdaten zugegriffen wird und diese abgerufen werden.

Aufgabe ist es auch hier, wie eingangs bereits erläutert, ein Verfahren anzugeben, welches erhöhte Datensicherheit und zugleich hohe Datenverwertbarkeit unter Wahrung der Anonymität der Objekte bietet.

Erfindungsgemäß wird dies dadurch erreicht, daß im Speicherschritt die Objektidentifikationsdaten und die Nutzdaten in der Objektdaten-Datenbank voneinander getrennt gespeichert werden, sodaß sie aus der Objektdaten-Datenbank getrennt abgerufen werden können, allein aus den gespeicherten Datensätzen jedoch kein Zusammenhang zwischen den Objektidentifikationsdaten und den Nutzdaten ableitbar ist,

- daß in einem Vergabeschritt Sicherheitsschlüssel an jede der Standard-Instanzen vergeben werden, die ein Zugreifen auf die Objektidentifikationsdaten und die zugehörigen Nutzdaten für jede der jeweiligen Standard-Instanzen ermöglichen, wobei gegebenenfalls für jede der Standard-Instanzen eine Wiedergewinnungs-Instanz definiert wird, über welche bei Verlust des Sicherheitsschlüssels dieser wieder erzeugt werden kann,

- daß jede der Standard-Instanzen weiteren Instanzen den vollen oder teilweisen Datenzugriff auf ihre Objektdaten gestatten kann,

- und daß in einem Abfrageschritt über eine der Standard-Instanzen oder gegebenenfalls eine Wiedergewinnungs-Instanz und/oder eine der weiteren Instanzen nach Eingabe des Sicherheitsschlüssels oder eines Teils davon auf die Objektidentifikationsdaten in Verbindung mit den zugehörigen Nutzdaten zugegriffen wird.

Allein über den Sicherheitsschlüssel ist die Zuordnung der getrennten Objektidentifikationsdaten und der Nutzdaten möglich. Dabei verbleibt der Sicherheitsschlüssel oder ein Teil davon bei der Standard-Instanz und kann bei Verlust oder Zerstörung über die Wiedergewinnungs-Instanz wiederhergestellt werden, um zu verhindern, daß die Zuordnung der Identifikationsdaten und Nutzdaten der Standard-Instanz für immer verloren sind. Da der Sicherheitsschlüssel bei der jeweiligen Standard-Instanz verbleibt, sind die für den Datenzugriff erforderlichen Schlüssel nicht zentral abrufbar und daher vor einer nicht-autorisierten Verwendung geschützt.

Auf welche Weise der Sicherheitsschlüssel aufbewahrt und verwaltet wird, bleibt dem Anwender überlassen. Es hat sich aber bewährt, zumindest einen Teil des Sicherheitsschlüssels durch eine Verschlüsselung im System zu hinterlegen, wobei auch die Wiedergewinnungs-Instanz eine solche Verschlüsselung vornehmen, damit sie den Sicherheitsschlüssel bei Bedarf zumindest teilweise generieren kann.

Eine Möglichkeit, eine Wiedergewinnungs-Instanz auszubilden, besteht darin, daß für jede Standard-Instanz zwei oder mehrere Systemoperator-Instanzen aus mehreren, voneinander unabhängigen Systemoperator-Instanzen ausgewählt werden, ohne daß den ausgewählten Systemoperator-Instanzen die Identität der jeweils anderen ausgewählten Systemoperator-Instanz(en) bekannt ist, daß der Sicherheitsschlüssel der jeweiligen Standard-Instanz auch an die zwei oder mehreren, ausgewählten Systemoperator-Instanzen vergeben wird, sowie den zumindest zwei ausgewählten Systemoperator-Instanzen für den gemeinsamen Zugriff zur Verfügung steht, und gegebenenfalls im Abfrageschritt über die zwei oder mehreren Systemoperator-

Instanzen nach gemeinsamer Eingabe des Sicherheitsschlüssels auf die Objektidentifikationsdaten in Verbindung mit den zugehörigen Nutzdaten zugegriffen wird. Um die Sicherheit weiter zu verbessern, ist es möglich, dass die ausgewählten Systemoperator-Instanz(en) räumlich getrennt voneinander tätig sind.

Die nach dem Zufallsprinzip bestimmten, zumindest zwei Systemoperator-Instanzen besitzen jeweils z.B. über einen Sicherheitsschlüssel die Möglichkeit, gemeinsam auf den inneren Teil eines Sicherheitsschlüssels einer Standard-Instanz zuzugreifen, um die Objektidentifikationsdaten und die Nutzdaten derselben abzufragen. Im Bedarfsfall können die ausgewählten Systemoperator-Instanzen über diese Zugriffsberechtigung auch die Vergabe eines neuen äußeren Teils des Sicherheitsschlüssels veranlassen, damit ein verloren gegangener Sicherheitsschlüssel auf diese Weise ersetzt werden kann.

Gemäß einer weiteren Ausführungsform der Erfindung kann weiters vorgesehen sein, daß zur Erstellung des Sicherheitsschlüssels von einer Logik für die Zuordnung von Objektidentifikationsdaten und Nutzdaten einer bestimmten Standard-Instanz ein innerer Schlüssel der jeweiligen Standard-Instanz generiert wird und an diese Standard-Instanz sowie an die zumindest zwei ausgewählten Systemoperator-Instanzen weitergeleitet wird, und daß der innere Schlüssel von dieser Standard-Instanz und von den Systemoperator-Instanzen mit jeweils einem äußeren Schlüssel verschlüsselt an die Objektdaten-Datenbank zurückgesendet und dort abgelegt wird.

Damit kann nur die Standard-Instanz oder die zumindest zwei Systemoperator-Instanzen zusammen über ihren privaten äußeren Schlüssel auf den inneren Schlüssel zugreifen, der wiederum die Entschlüsselung des Zusammenhanges zwischen Objektidentifikationsdaten und Nutzdaten der betreffenden Standard-Instanz ermöglicht. Die Systemoperator-Instanzen, die idealerweise keine Kenntnis ihrer gegenseitigen Berechtigungen haben, können bei einer Anfrage nur feststellen, daß sie zusammen mit einer oder mehreren anderen Systemoperator-Instanzen dazu ausgewählt sind, für eine ihnen unbekannte Standard-Instanz den inneren Schlüssel durch Eingabe ihres privaten äußeren Schlüssels zu entschlüsseln und

damit den Zugang zu den Objektidentifikationsdaten und den Nutzdaten für diese Standard-Instanz zu ermöglichen.

Nachfolgend wird die Erfindung anhand der in den Zeichnungen dargestellten Ausführungsbeispiele eingehend erläutert. Es zeigt dabei

Fig.1 ein Blockschaltbild einer Ausführungsform des erfindungsgemäßen Datenverarbeitungssystems;
Fig.2 ein Blockschaltbild einer weiteren Ausführungsform des erfindungsgemäßen Datenverarbeitungssystems;
Fig.3 eine schematische Darstellung eines Zugriffs-Schichtenmodells in Zusammenhang mit dem Aufbau eines Sicherheitsschlüssels;
Fig.4 den schematischen Ablauf zur Vergabe eines Sicherheitsschlüssels gemäß einer Ausführungsform des erfindungsgemäßen Verfahrens;
Fig.5 den schematischen Ablauf zur Herausgabe eines vorhandenen Sicherheitsschlüssels an eine bestehende Instanz gemäß einer weiteren Ausführungsform des erfindungsgemäßen Verfahrens;
Fig.6 den schematischen Ablauf zum Hinzufügen neuer Nutzdaten gemäß einer weiteren Ausführungsform des erfindungsgemäßen Verfahrens;
Fig.7 den schematischen Ablauf zum Lesen vorhandener Nutzdaten gemäß einer weiteren Ausführungsform des erfindungsgemäßen Verfahrens;
Fig.8 den schematischen Ablauf zum Hinzufügen einer Assoziierten Instanz und
Fig.9 den schematischen Ablauf zum Hinzufügen einer Autorisierten Instanz

Fig.1 zeigt ein Datenverarbeitungssystem zur Verarbeitung von Objektdaten einer Standard-Instanz 101, welche stellvertretend für eine Person, ein System, einen Dateninhaber od. dgl. dargestellt ist. In dem in Fig.1 gezeigten Beispiel stellt die Standard-Instanz 101 als Objektdaten Personendaten bereit oder entnimmt diese

einer als Personendaten-Datenbank 20 betriebenen Objektdaten-Datenbank, in welcher die Personendaten über Zugriffseinrichtungen 70 speicherbar oder abrufbar sind. In der Personendaten-Datenbank 20 können Daten von einer Vielzahl von Standard-Instanzen abgelegt sein.

Die in weiterer Folge als Beispiel dienende Verarbeitung von Patientendaten ist nicht als einschränkend zu verstehen, vielmehr können im Rahmen der Erfindung auch andere Arten von Daten, beispielsweise Dokumente in einem Unternehmen, bearbeitet werden, nicht nur die von Patienten.

Die Personendaten umfassen Objektidentifizierungsdaten, nämlich Personenidentifikationsdaten 100 und zugehörige Nutzdaten 110, wobei die Personenidentifikationsdaten Daten beinhalten, die eine Person, z.B. einen Patienten identifizieren, also etwa Sozialversicherungsnummer, Name, Geburtsdatum, Wohnort, Staatsbürgerschaft usw.

Getrennt von diesen Personenidentifikationsdaten sind die Nutzdaten 110 gespeichert, welche verschiedene Einträge und aufgezeichnete Anamnese Daten umfassen können, z.B. Röntgenaufnahmen, Mammographie-Daten, NMR-Daten, die für Diagnosen benötigt und eine bestimmte Zeit gespeichert werden können oder müssen.

Die Zugriffseinrichtungen sind in Fig.1 als zentrale Logik 70 dargestellt, die eine Vielzahl von Eingabe- und Ausgabevorrichtungen und eine Steuereinrichtung beinhaltet und eine Schnittstelle zwischen der Personendaten-Datenbank 20 und Instanzen 101, 60, 50 und 40 darstellt, die Personendaten speichern oder abfragen.

Erfindungsgemäß sind die Personenidentifikationsdaten 100 und die Nutzdaten 110 in der Personendaten-Datenbank 20 voneinander getrennt speicherbar und abrufbar, sodaß allein aus den gespeicherten Datensätzen kein Zusammenhang zwischen den Objektidentifikationsdaten und den Nutzdaten ableitbar ist. Dies kann durch die

Zugriffssteuerung (logisch) sowie durch räumlich getrenntes (physikalisch) Vorsehen von zwei Datenbanken geschehen.

Der Zugriff auf Personenidentifikationsdaten 100 in Verbindung mit den zugehörigen Nutzdaten 110 ist nur nach Eingabe eines Sicherheitsschlüssels gestattet, der für die jeweilige Standard-Instanz 101 vergeben ist, welche durch die Personenidentifikationsdaten 100 identifiziert ist. Wenn für eine Standard-Instanz 101 z.B. im Rahmen einer Untersuchung Daten aufgezeichnet werden, so erhält die Standard-Instanz 101 vom erfindungsgemäßen Datenverarbeitungssystem einen für diese Standard-Instanz 101 vergebenen Sicherheitsschlüssel, welcher ganz oder teilweise auf einem Sicherheits-Token gespeichert ist, z.B. auf einer Smartcard mit PIN-Kode od. dgl.

Somit kann die Standard-Instanz 101 unter Eingabe des Sicherheitsschlüssels auf die eigenen Nutzdaten 110 zugreifen, während andere Standard-Instanzen vom Zugriff ausgeschlossen sind. Damit ist sichergestellt, daß die gespeicherten Nutzdaten 110, z.B. Krankengeschichten, durch Außenstehende nicht mit einer konkreten Standard-Instanz 101 in Zusammenhang gebracht werden können.

Wie erwähnt können weitere Instanzen im erfindungsgemäßen Datenverarbeitungssystem zugelassen werden, denen andere Berechtigungen ermöglicht werden. So kann z.B. eine Forschungs-Instanz 40 vorgesehen sein, die zum Zwecke der Analyse ausschließlich Zugriff auf die Nutzdaten 110 hat. Dadurch kann in sinnvoller Weise auf die Nutzdaten 110 zugegriffen werden und diese für statistische Untersuchungen und Studien, z.B. zur Verbesserung der medizinischen Behandlung oder zu Diagnosezwecken, Verwendung finden ohne die Identität der Patienten preisgeben zu müssen. Durch die vollkommene Trennung der Personenidentifikationsdaten 100 und der Objektdaten 110 können Rückschlüsse aus den Nutzdaten 110 auf die Personenidentifikationsdaten 100 verhindert werden und die Anonymität der Standard-Instanzen bleibt gewahrt.

Es kann vorkommen, daß die Standard-Instanz 101 ihr Sicherheits-Token mit dem darauf abgelegten Sicherheitsschlüssel verliert oder zerstört. Um zu verhindern, daß die gespeicherten Nutzdaten 110 der jeweiligen Standard-Instanz 101 unwiederbringlich verlorengehen, weil die Zuordnung der Personendaten der Standard-Instanz 101 zu den Nutzdaten nicht mehr vorhanden wäre, kann für jede der Standard-Instanzen eine bzw. mehrere Wiedergewinnungs-Instanzen außerhalb der Objektdaten-Datenbank 20 definiert werden.

Im Ausführungsbeispiel gemäß Fig.1 sind als Wiedergewinnungs-Instanz mehrere voneinander unabhängige Systemoperator-Instanzen 30 vorhanden, aus denen jeweils zwei oder mehrere Systemoperator-Instanzen für eine zugeordnete Standard-Instanz auswählbar sind, ohne daß den ausgewählten Systemoperator-Instanzen die Identität der jeweils anderen ausgewählten Systemoperator-Instanz(en) oder der Standard-Instanzen bekannt ist, wobei der an die zugeordnete Standard-Instanz 101 vergebene Sicherheitsschlüssel den zumindest zwei ausgewählten Systemoperator-Instanzen zumindest teilweise zugänglich ist, sodaß ein gemeinsamer Zugriff auf die Personenidentifikationsdaten 100 in Verbindung mit den zugehörigen Nutzdaten 110 für die zugeordnete Standard-Instanz 101 ermöglicht ist.

Um die Unabhängigkeit der zumindest zwei Systemoperator-Instanzen sicherzustellen, sind diese für jede Standard-Instanz 101 an unterschiedlichen Orten vorgesehen und es wird ihnen die gegenseitige Zuordnung nicht bekanntgegeben.

Wenn einer der ausgewählten Systemoperator-Instanzen das System verlässt, kann der Sicherheitsschlüssel bzw. Teile des Sicherheitsschlüssels der Standard-Instanz 101 vorher erzeugt und an eine andere Systemoperator-Instanz weitergegeben werden.

Beim erfindungsgemäßen Verfahren zur Verarbeitung von Objektdaten, hier Personendaten einer Standard-Instanz 101 werden in einem Speicherschritt die Personendaten in der Personendaten-Datenbank 20 gespeichert und in einem

Abfrageschritt aus der Personendaten-Datenbank 20 auf die Personendaten zugegriffen.

Im Speicherschritt werden die Personenidentifikationsdaten 100 und die Nutzdaten 110 in der Personendaten-Datenbank 20 voneinander getrennt gespeichert, sodaß sie aus der Personendaten-Datenbank 20 getrennt abgerufen werden können. Allein aus den gespeicherten Datensätzen ist jedoch – wie bereits vorstehend erwähnt - kein Zusammenhang zwischen den Personenidentifikationsdaten 100 und den Nutzdaten 110 ableitbar.

Weiters werden im Vergabeschritt Sicherheitsschlüssel an jede der Standard-Instanzen 101 vergeben und für jede Standard-Instanz 101 eine Wiedergewinnungs-Instanz definiert, indem zwei oder mehrere Systemoperator-Instanzen aus mehreren, voneinander unabhängigen Systemoperator-Instanzen 30 ausgewählt werden, ohne daß den ausgewählten Systemoperator-Instanzen die Identität der jeweils anderen ausgewählten Systemoperator-Instanz(en) sowie der Standard-Instanz 101 selbst bekannt ist, wobei der Sicherheitsschlüssel der jeweiligen Standard-Instanz 101 zumindest teilweise auch an die zwei oder mehreren, ausgewählten Systemoperator-Instanzen vergeben wird.

Das Vorsehen einer Wiedergewinnungs-Instanz ist nicht zwingend erforderlich, schützt aber vor dem völligen Datenverlust für eine Standard-Instanz 101, wenn der zugehörige Sicherheitsschlüssel verloren gehen sollte.

Im Abfrageschritt wird über die Standard-Instanz nach Eingabe des Sicherheitsschlüssels auf die Personen-Identifikationsdaten 100 in Verbindung mit den zugehörigen Nutzdaten 110 zugegriffen, und gegebenenfalls wird über die zwei oder mehreren Systemoperator-Instanzen nach gemeinsamer Eingabe des Sicherheitsschlüssels auf die Personen-Identifikationsdaten 100 in Verbindung mit den zugehörigen Nutzdaten 110 zugegriffen.

Der Sicherheitsschlüssel oder ein Teil davon verbleibt bei der Standard-Instanz 101 und gegebenenfalls weiteren von der Standard-Instanz 101 autorisierten Instanzen 50, 60 und steht bei dem Einsatz der Systemoperatoren als eine der optionalen Wiedergewinnungs-Instanzen den zumindest zwei ausgewählten Systemoperator-Instanzen 30 für den gemeinsamen Zugriff zur Verfügung.

In einer Weiterbildung des erfindungsgemäßen Datenverarbeitungssystems können verschiedene Instanzen definiert sein, z.B. eine Standard-Instanz, eine assoziierte Instanz und eine autorisierte Instanz.

Die Standard-Instanz ist dabei die Inhaberin der Nutzdaten und hat unlimitierte Rechte, anderen Personen oder Instanzen den Zugriff auf die Nutzdaten zu gestatten. Die assoziierte Instanz wird durch die Standard-Instanz autorisiert und hat ebenfalls unbegrenzten Zugriff auf alle Daten der Standard-Instanz sowie die Berechtigung, weitere Instanzen zu autorisieren. Demgegenüber ist die autorisierte Instanz nur berechtigt, auf definierte Einträge der Datenbank 20 zuzugreifen, entsprechend der Autorisierung durch die Standard-Instanz oder die assoziierte Instanz. Weiters kann die assoziierte Instanz als Wiedergewinnungs-Instanz eingesetzt werden.

Im Ausführungsbeispiel gemäß Fig.2 sind die Systemkomponenten so angeordnet, daß die jeweiligen Instanzen 101, 50, 60 sowie 40 ohne der in Fig.1 zwischengeschalteten Logik Zugriff auf die Objektdaten-Datenbank 20 hat. Die Logik wird somit dezentral realisiert.

Zur Erstellung des Sicherheitsschlüssels wird von der Logik 70 oder der Personendaten-Datenbank 20 für die Zuordnung von Personenidentifikationsdaten 100 und Nutzdaten 110 einer bestimmten Standard-Instanz 101 ein innerer Schlüssel der jeweiligen Standard-Instanz generiert und an diese Standard-Instanz 101 sowie optional an eine oder mehrere Wiedergewinnungs-Instanzen weitergeleitet. Der Sicherheitsschlüssel wird von dieser Standard-Instanz 101 und den

Wiedergewinnungs-Instanzen mit jeweils einem äußeren Schlüssel verschlüsselt an die Objektdaten-Datenbank 20 zurückgesendet und dort abgelegt.

Der Sicherheitsschlüssel kann zwei- oder mehrteilig ausgebildet sein, sodaß ein äußerer Schlüssel bei der Standard-Instanz verbleibt und über diesen auf einen nächstinneren Schlüssel zugegriffen bzw. dieser durch Entschlüsselung zugänglich gemacht werden kann. Dieser nächstinnere Schlüssel kann wiederum auf den seinerseits nächstinneren Schlüssel zugreifen, usw. Auf diese Weise können Zugriffsberechtigungen je nach Anzahl der verwendeten Schichten verschiedenartig festgelegt werden.

Bei Verlust des äußeren Schlüssels durch die Standard-Instanz kann z.B. eine weitere Instanz berechtigt sein kann, auf den nächstinneren Schlüssel zuzugreifen bzw. diesen durch Entschlüsselung zugänglich zu machen. Der Datenzugriff wird durch Entschlüsselung bis zur innersten Schicht ermöglicht, wonach wieder ein neuer äußerer Schlüssel gebildet werden kann, welcher der betroffenen Instanz zur Verfügung gestellt wird.

Fig.3 zeigt ein zur Umsetzung der Erfindung verwendbares Zugriffs-Schichtenmodell. Es ist eine äußere Schicht 200 und eine innere Schicht 201 ausgebildet.

Die Standard-Instanz 101 gibt den äußeren Schlüssel 90 der äußeren Schicht 200 ein und entschlüsselt damit in der inneren Schicht 201 den inneren Schlüssel K_{S0}^{-1} der Standard-Instanz 101, der wiederum den Zugriff auf die Nutzdaten CD der Standard-Instanz 101 mit der Nutzdatenidentifikation CID ermöglicht.

Zugleich verfügt die assoziierte Instanz 60 über einen äußeren Schlüssel 91, der seinen inneren Schlüssel K_{A0}^{-1} entschlüsselt, welcher hiermit Zugriff auf den inneren Schlüssel K_{S0}^{-1} der Standard-Instanz 101 bietet. Ändert die Standard-Instanz 101 ihre inneren Schlüssel kann sie jederzeit einen weiteren Zugriff durch die assoziierte

Instanz und die Systemoperator-Instanzen verhindern. Der äußere Schlüssel der Standard-Instanz kann dabei aber beibehalten werden.

Die beiden Systemoperator-Instanzen 30 entschlüsseln den inneren Schlüssel K_{S0}^{-1} der Standard-Instanz 101 mit ihren jeweiligen inneren Schlüsseln K_{O0}^{-1}, der wiederum durch ihre äußeren Schlüssel 93, 94 entschlüsselt wird.

Für die autorisierte Instanz 50 liegt nur die Berechtigung für den Zugriff auf bestimmte Datensätze vor, die über den äußeren Schlüssel 92 und den inneren Schlüssel K_{A0}^{-1} realisiert wird.
Wenn im Rahmen der Erfindung von einem äußeren und einem inneren Schlüssel die Rede ist, so können diese vorzugsweise jeweils aus einem privaten und einem öffentlichen Schlüssel gebildet sein, wodurch die Flexibilität erhöht wird.

Fig.4 zeigt den Ablauf im erfindungsgemäßen Datenverarbeitungssystem für das Hinzufügen einer neuen Standard-Instanz 101. Folgende Schritte werden dabei ausgeführt, welche in Fig.4 schematisch wiedergegeben sind:

Schritt (1): Die neue Standard-Instanz 101 identifiziert sich gegenüber der Logik 70 bzw. einer autorisierten Person.

Schritt (2): Die Personenidentifikationsdaten (SID) der Standard-Instanz 101 werden von der Logik 70 an die Datenbank 20 gesendet.

Schritt (3): Die Datenbank 20 meldet, daß die angegebene SID unbekannt ist.

Schritt (4): Die Logik 70 generiert für die hinzuzufügende Standard-Instanz einen neuen Sicherheits-Schlüssel, der ein Schlüsselpaar aus einem inneren Schlüssel sowie einem äußeren Schlüssel umfasst, und überträgt den privaten inneren Schlüssel K_{S0}^{-1} verschlüsselt mit dem äußeren öffentlichen Schlüssel K_S der Standard-Instanz 101 zur Datenbank 20.

Schritt (5): Die Logik 70 überträgt den inneren privaten Schlüssel K_{S0}^{-1} der Standard-Instanz 101 nacheinander verschlüsselt mit zwei oder mehreren äußeren öffentlichen Schlüsseln K_{O0} der Systemoperator-Instanzen 30 zur Datenbank 20. Damit steht der innere private Schlüssel K_{S0}^{-1} der Standard-Instanz 101 den ausgewählten Standard-Instanzen gemeinsam zur Verfügung, wenn diese ihre inneren privaten Schlüssel anwenden, um den inneren privaten Schlüssel K_{S0}^{-1} der Standard-Instanz 101 zu entschlüsseln.

Eine zweite Möglichkeit ist, daß der innere private Schlüssel K_{S0}^{-1} der Standard-Instanz 101 aufgeteilt wird und mit den jeweiligen öffentlichen Schlüsseln K_{O0} der Systemoperator-Instanzen 30 verschlüsselt in der Datenbank 20 gespeichert wird.

Schritt (6): Die Logik 70 überträgt den inneren öffentlichen Schlüssel K_{S0} der Standard-Instanz 101 zur Datenbank 20. Auf diese Weise können Daten der Standard-Instanz 101 mit dem Schlüssel K_{S0} verschlüsselt werden.

Schritt (7): Die Logik 70 überträgt den äußeren öffentlichen Schlüssel K_S der Standard-Instanz 101 zur Datenbank 20.

Schritt (8): Die Logik 70 überträgt die Personenidentifikationsdaten (SID) der Standard-Instanz 101 verschlüsselt mit den inneren öffentlichen Schlüsseln K_{O0} der Systemoperatoren 30 zur Datenbank 20.

Schritt (9): Die Logik 70 übergibt den äußeren privaten Schlüssel 90 (z.B. zur Speicherung auf einer Smartcard) an die entsprechende Standard-Instanz 101. Der äußere Schlüssel 90 ist somit Teil des Sicherheitsschlüssels und wird zum Zugriff auf den inneren Schlüssel der Standard-Instanz benötigt. Alternativ kann die Logik 70 die Verbindung zwischen den ausgewählten Systemoperatoren 30 und der zugehörigen Standard-Instanz 101 auch selbst verschlüsseln und so geheimhalten.

Sobald der Sicherheitsschlüssel an die Standard-Instanz 101 vergeben worden ist, bleibt er über seine gesamte Lebensdauer der Standard-Instanz im System einmalig vorhanden, oder die Standard-Instanz 101 entscheidet sich, ihn zu ändern.

Fig.5 beschreibt den Ablauf zur Herausgabe eines neuen äußeren Sicherheitsschlüssels an eine bestehende Standard-Instanz. Folgende Schritte werden dabei ausgeführt, welche in Fig.5 schematisch wiedergegeben sind:

Schritt (1): Die Standard-Instanz 101 identifiziert sich gegenüber der Logik 70 bzw. einer autorisierten Person.

Schritt (2): Die Standard-Instanz 101 sendet ihre Personenidentifikationsdaten (SID) an die Logik 70.

Schritt (3): Die Logik 70 sendet die Personenidentifikationsdaten (SID) der Standard-Instanz 101 an die Datenbank 20.

Schritt (4): Die Datenbank 20 antwortet mit der Übermittlung aller den Systemoperatoren 30 zugewiesenen Personenidentifikationsdaten (SIDs).

Schritt (5): Die Logik 70 sendet die gewünschten Personenidentifikationsdaten (SID) der Standard-Instanz 101 sowie die den Systemoperatoren 30 zugewiesenen Personenidentifikationsdaten (SIDs) verschlüsselt mit dem inneren öffentlichen Schlüssel K_{O0} des jeweiligen Systemoperators 30 an alle Systemoperatoren 30. Diese entschlüsseln ihre zugewiesenen Personenidentifikationsdaten (SIDs) mit ihrem inneren privaten Schlüssel K_{O0}^{-1} und stellen durch Vergleich mit den gewünschten Personenidentifikationsdaten (SID) der Standard-Instanz 101 fest, ob sie für die jeweilige Standard-Instanz 101 zuständig sind.

Optional können die zugewiesenen Personenidentifikationsdaten (SIDs) zusätzlich mit dem öffentlichen Schlüssel K_{L0} der Logik verschlüsselt sein. In diesem Fall

können die Systemoperatoren 30 nicht feststellen, ob sie einer Standard-Instanz 101 zugeordnet sind. Es folgt daher die Übermittlung der einfach entschlüsselten zugewiesenen Personenidentifikationsdaten (SIDs) an die Logik 70.

Schritt (6): Die Systemoperatoren 30 benachrichtigen die Logik 70 über ihre Zuständigkeit betreffend der Standard-Instanz 101.

Optional können die Systemoperatoren 30 der Logik 70 auch die mit dem jeweiligen Systemoperator-Schlüssel entschlüsselten, aber noch mit dem öffentlichen Schlüssel K_{L0} der Logik 70 verschlüsselten SIDs übermitteln. In diesem Fall entschlüsselt die Logik 70 die SIDs mit dem privaten Schlüssel K_{L0}^{-1} der Logik 70 und stellt durch Vergleich mit den gewünschten Personenidentifikationsdaten (SID) der Standard Instanz 101 fest, welche Systemoperator-Instanzen 30 welcher Standard-Instanz 101 zugeordnet sind.

Schritt (7): Die Logik 70 sendet die Liste der zuständigen Systemoperatoren 30 an die Datenbank 20.

Schritt (8): Die Datenbank 20 übermittelt den inneren privaten Schlüssel K_{S0}^{-1} der Standard-Instanz 101 nacheinander verschlüsselt mit zwei oder mehreren öffentlichen Systemoperator-Instanz 30-Schlüsseln K_{O0} zur Logik 70.

Eine zweite Möglichkeit ist, daß der innere private Schlüssel K_{S0}^{-1} der Standard-Instanz 101 aufgeteilt wurde und mit den jeweiligen öffentlichen Schlüsseln K_{O0} der Systemoperator-Instanzen 30 verschlüsselt übertragen wird.

Schritt (9): Die Logik 70 überträgt den inneren privaten Schlüssel K_{S0}^{-1} der Standard-Instanz 101 nacheinander verschlüsselt mit zwei oder mehreren öffentlichen Schlüsseln K_{O0} der Systemoperatoren-Instanzen 30 zu den jeweilig zuständigen Systemoperatoren-Instanzen 30.

Eine zweite Möglichkeit ist, daß der Schlüssel K_{S0}^{-1} der Standard-Instanz 101 aufgeteilt wurde und mit den jeweiligen öffentlichen Schlüsseln K_{O0} der Systemoperator-Instanzen 30 verschlüsselt übertragen wird.

Schritt (10): Die Logik 70 sendet den neuen äußeren öffentlichen Schlüssel $K_{S'}$ der Standard-Instanz 101 an die jeweilig zuständigen Systemoperator-Instanzen 30.

Schritt (11): Die jeweilig zuständigen Systemoperator-Instanzen 30 entschlüsseln nacheinander den inneren privaten Schlüssel K_{S0}^{-1} der Standard-Instanz 101 mit ihren jeweiligen inneren privaten Schlüsseln K_{O0}^{-1} und verschlüsseln den inneren privaten Schlüssel K_{S0}^{-1} der Standard-Instanz 101 mit dem äußeren öffentlichen Schlüssel $K_{S'}$ der Standard-Instanz 101 und übertragen diesen an die Logik 70. Optional ist es hier möglich, daß zusätzlich eine Verschlüsselung mit dem Schlüssel K_{L0} der Logik 70 vorgenommen wird, um die Schlüssel auch vor den Systemoperator-Instanzen geheim zu halten.

Eine zweite Möglichkeit ist, daß der Schlüssel K_{S0}^{-1} der Standard-Instanz 101 aufgeteilt wird und mit den jeweiligen öffentlichen Schlüssel K_{O0} der Systemoperator-Instanzen 30 verschlüsselt in der Datenbank 20 gespeichert wird

Schritt (12): Die Logik 70 übergibt den mit dem neuen äußeren öffentlichen Schlüssel $K_{S'}$ der Standard-Instanz 101 verschlüsselten inneren privaten Schlüssel K_{S0}^{-1} der Standard-Instanz 101 an die Datenbank 20.

Schritt (13): Die Logik 70 ersetzt den bisher gültigen äußeren öffentlichen Schlüssel K_S der Standard-Instanz 101 durch den neuen äußeren öffentlichen Schlüssel $K_{S'}$ der Standard-Instanz 101.

Schritt (14): Die Logik 70 übergibt den äußeren privaten Sicherheitsschlüssel 90 (z.B. Smartcard) an die entsprechende Standard-Instanz 101.

Für die Eintragung von Nutzdaten 110 in der Personendaten-Datenbank 20 werden weitere Sicherheitsschlüssel generiert, die mit dem inneren öffentlichen Schlüssel der Standard-Instanz verschlüsselt werden, wobei gegebenenfalls die weiteren Sicherheitsschlüssel mit dem inneren öffentlichen Schlüssel der autorisierten Instanz verschlüsselt werden.

Auf diese Weise kann kein direkter Zusammenhang zwischen den Nutzdaten 110 und der Standard-Instanz 101 hergestellt werden, indem über bestimmte Eigenschaften der Standard-Instanz 101, z.B. über den Verlauf einer Krankheit, Rückschlüsse gezogen werden. Damit wird das Erstellen von Profilen über die Standard-Instanzen wirkungsvoll verhindert. Der weitere Sicherheitsschlüssel wird vorzugsweise von Zeit zu Zeit oder nach einer bestimmten Anzahl an Nutzdaten-Einträgen verändert.

Fig.6 beschreibt den Ablauf zum Hinzufügen neuer Nutzdaten. Folgende Schritte werden dabei ausgeführt, welche in Fig.6 schematisch wiedergegeben sind:

Schritt (1): Die Standard-Instanz 101 meldet sich im System durch Eingabe des Sicherheitsschlüssels an, indem z.B. ein PIN-Code eingegeben wird, um sich gegenüber einer Smartcard 90 zu authentifizieren.

Schritt (2): Die Standard-Instanz 101 übermittelt ihre Personenidentifikationsdaten (SID) an die Logik 70. Im gleichen Schritt wird der Standard-Instanz 101 auch der öffentliche Schlüssel der Logik 70 K_{L0} bekannt gegeben.

Schritt (3): Die Standard-Instanz 101 übermittelt neue Nutzdaten (CD) an die Logik 70.

Schritt (4): Die Standard-Instanz 101 übermittelt eine indizierende Kennzeichnung ID (z.B. Suchbegriffe, Datum, etc.) verschlüsselt mit dem öffentlichen Schlüssel der Logik K_{L0} an die Logik 70.

Schritt (5): Die Logik überträgt die Personenidentifikationsdaten (SID) der Standard-Instanz 101 an die Datenbank 20.

Schritt (6): Falls ein neuer Schlüssel erzeugt werden muss, informiert die Datenbank 20 die Logik 70.

Schritt (7): Die Logik 70 erzeugt einen neuen Nutzdaten-Schlüssel K_{Si} und verschlüsselt diesen mit dem inneren öffentlichen Schlüssel K_{S0} der Standard-Instanz 101 und übermittelt diesen an die Datenbank 20.

Schritt (8): Danach verschlüsselt die Logik 70 die Personenidentifikationsdaten (SID) der Standard-Instanz 101 mit dem Nutzdaten-Schlüssel K_{Si} und überträgt sie zur Datenbank 20. Dieses Merkmal wird als Nutzdaten-Identifikationscode (CID) bezeichnet.

Schritt (9): Danach entschlüsselt die Logik 70 die gewählte indizierende Kennzeichnung (z.B. Suchbegriffe, Datum, etc.) der Standard-Instanz 101 mit dem privaten Schlüssel der Logik K_{L0}^{-1} und verschlüsselt die Kennzeichnung (ID) mit dem inneren öffentlichen Schlüssel K_{S0} der Standard-Instanz 101.

Schritt (10): Abschließend überträgt die Logik 70 die Nutzdaten (CD) zur Datenbank 20 und bindet sie an die zuvor gebildeten Identifikationsdaten.

Fig.7 beschreibt den Ablauf zum Lesen vorhandener Nutzdaten. Folgende Schritte werden dabei ausgeführt, welche in Fig.7 schematisch wiedergegeben sind:

Schritt (1): Die Standard-Instanz 101 meldet sich im System durch Eingabe des Sicherheitsschlüssels an, indem z.B. ein PIN-Code eingegeben wird, um sich gegenüber einer Smartcard 90 zu authentifizieren.

Schritt (2): Die Standard-Instanz 101 übermittelt ihre Personenidentifikationsdaten (SID) an die Logik 70.

Schritt (3): Die Logik 70 übermittelt die Personenidentifikationsdaten (SID) der Standard-Instanz 101 an die Datenbank 20.

Schritt (4): Die Datenbank 20 übermittelt alle indizierenden Kennzeichnungen (CIDs) verschlüsselt mit dem inneren öffentlichen Schlüssel K_{S0} der Standard-Instanz 101 an die Logik 70.

Schritt (5): Die Logik 70 übermittelt alle indizierenden Kennzeichnungen (CIDs) verschlüsselt mit dem inneren öffentlichen Schlüssel K_{S0} der Standard-Instanz an die Standard-Instanz 101.

Schritt (6): Die Standard-Instanz 101 entschlüsselt ihren inneren privaten Schlüssel K_{S0}^{-1} mit ihrem äußeren privaten Schlüssel K_S^{-1}. Anschließend benutzt sie den inneren privaten Schlüssel K_{S0}^{-1}, um die verschlüsselten indizierenden Kennzeichnungen (CIDs) zu entschlüsseln und eine Kennzeichnung (ID) sowie einen zugehörigen Nutzdaten-Schlüssel K_{Si} auszuwählen. Danach verschlüsselt sie ihre Personenidentifikationsdaten (SID) mit dem zur entsprechenden indizierten Kennzeichnung assoziierten Nutzdaten-Schlüssel K_{Si} und übermittelt den daraus resultierende Nutzdaten-Identifikationscode (CID) an die Logik 70.

Schritt (7): Die Logik 70 sendet den Nutzdaten-Identifikationscode an die Datenbank 20.

Schritt (8): Die Datenbank 20 sendet die Nutzdaten an die Logik 70.

Schritt (9): Die Logik übermittelt die Nutzdaten an die Standard-Instanz 101.

Fig.8 beschreibt den Ablauf zum Hinzufügen einer assoziierten Instanz. Folgende Schritte werden dabei ausgeführt, welche in Fig.8 schematisch wiedergegeben sind:

Schritt (1a, 1b): Die Standard-Instanz 101 und die assoziierte Instanz 60 melden sich im System durch Eingabe des Sicherheitsschlüssels an, indem z.B. ein PIN-Code eingegeben wird, um sich gegenüber einer Smartcard 90 zu authentifizieren.

Schritt (2): Die Personenidentifikationsdaten (SID) der Standard-Instanz 101 werden von der Standard-Instanz 101 an die Logik 70 übermittelt.

Schritt (3): Die Logik 70 sendet die Personenidentifikationsdaten (SID) der Standard-Instanz 101 an die Datenbank 20.

Schritt (4): Die assoziierte Instanz 60 übermittelt ihre Personenidentifikationsdaten (AID) an die Logik 70.

Schritt (5): Die Logik 70 übermittelt die Personenidentifikationsdaten (AID) der assoziierten Instanz 60 an die Datenbank 20.

Schritt (6): Die Datenbank 20 übermittelt den inneren öffentlichen Schlüssel K_{S0} der Standard-Instanz 101 an die Logik 70.

Schritt (7): Die Datenbank 20 übermittelt den inneren öffentlichen Schlüssel K_{A0} der assoziierten Instanz 60 an die Logik 70.

Schritt (8): Die Datenbank 20 sendet den inneren privaten Schlüssel K_{S0}^{-1} der Standard-Instanz 101 verschlüsselt mit dem äußeren öffentlichen Schlüssel K_S der Standard-Instanz 101 an die Logik 70.

Schritt (9): Die Logik 70 sendet den inneren privaten Schlüssel K_{S0}^{-1} der Standard-Instanz 101 verschlüsselt mit dem äußeren öffentlichen Schlüssel K_S der Standard-Instanz 101 an die Standard-Instanz 101.

Schritt (10): Die Logik 70 sendet den inneren öffentlichen Schlüssel K_{A0} der assoziierten Instanz 60 an die Standard-Instanz 101.

Schritt (11): Die Standard-Instanz 101 entschlüsselt ihren inneren privaten Schlüssel K_{S0}^{-1} mit ihrem äußeren privaten Schlüssel K_S^{-1} und verschlüsselt ihren inneren privaten Schlüssel K_{S0}^{-1} mit dem inneren öffentlichen Schlüssel K_{A0} der assoziierten Instanz 60 und übermittelt diesen an die Logik 70.

Schritt (12): Die Logik 70 sendet den inneren privaten Schlüssel K_{S0}^{-1} verschlüsselt mit dem inneren öffentlichen Schlüssel K_{A0} der assoziierten Instanz 60 an die Datenbank 20.

Schritt (13): Die Logik 70 sendet die Personenidentifikationsdaten (SID) der Standard-Instanz 101 verschlüsselt mit dem inneren öffentlichen Schlüssel K_{A0} der assoziierten Instanz 60 an die Datenbank 20.

Schritt (14): Die Logik 70 sendet die Personenidentifikationsdaten (AID) der assoziierten Instanz 60 verschlüsselt mit dem inneren öffentlichen Schlüssel K_{S0} der Standard-Instanz 101 an die Datenbank 20.

Fig.9 beschreibt den Ablauf zum Hinzufügen einer autorisierten Instanz 50. Folgende Schritte werden dabei ausgeführt, welche in Fig.9 schematisch wiedergegeben sind:

Schritt (1): Die Standard-Instanz 101 und die autorisierte Instanz 50 melden sich im System durch Eingabe des Sicherheits-Tokens an, indem z.B. ein PIN-Code eingegeben wird, um sich gegenüber einer Smartcard 90 zu authentifizieren. Im gleichen Schritt wird der Standard-Instanz 101 auch der öffentliche Schlüssel der Logik K_{L0} bekanntgegeben.

Schritt (2): Die Personenidentifikationsdaten (SID) der Standard-Instanz 101 werden von der Standard-Instanz an die Logik 70 übermittelt.

Schritt (3): Die Logik 70 sendet die Personenidentifikationsdaten (SID) der Standard-Instanz 101 an die Datenbank 20.

Schritt (4): Die autorisierte Instanz 50 übermittelt ihre Personenidentifikationsdaten (BID) an die Logik 70.

Schritt (5): Die Logik übermittelt die Personenidentifikationsdaten (BID) der autorisierten Instanz 50 an die Datenbank 20.

Schritt (6): Falls ein neuer Schlüssel erzeugt werden muss, informiert die Datenbank 20 die Logik 70.

Schritt (7): Die Datenbank 20 übermittelt den inneren öffentlichen Schlüssel K_{S0} der Standard-Instanz 101 an die Logik 70.

Schritt (8): Die Datenbank 20 übermittelt den inneren öffentlichen Schlüssel K_{B0} der autorisierten Instanz 50 an die Logik 70.

Schritt (9): Die Datenbank 20 übermittelt alle indizierenden Kennzeichnungen (CIDs) verschlüsselt mit dem inneren öffentlichen Schlüssel K_{S0} der Standard-Instanz 101 an die Logik 70.

Schritt (10): Die Logik 70 übermittelt alle indizierenden Kennzeichnungen (CIDs) verschlüsselt mit dem inneren öffentlichen Schlüssel K_{S0} der Standard-Instanz 101 an die Standard-Instanz 101.

Schritt (11): Die Standard-Instanz 101 übermittelt eine indizierende Kennzeichnung inklusive zugehörigem Nutzdaten-Schlüssel K_{Si} (z.B. Suchbegriffe, Datum, etc.) verschlüsselt mit dem öffentlichen Schlüssel K_{L0} an die Logik 70.

Schritt (12): Danach entschlüsselt die Logik 70 die gewählte indizierende Kennzeichnung (z.B. Suchbegriffe, Datum, etc.) der Standard-Instanz 101 mit dem privaten Schlüssel der Logik K_{L0}^{-1} und verschlüsselt die Kennzeichnung mit dem inneren öffentlichen Schlüssel K_{B0} der autorisierten Instanz 50 und überträgt diese zur Datenbank 20.

Schritt (13): Anschließend verschlüsselt die Logik 70 den gewählten Nutzdaten-Schlüssel K_{Si} mit dem inneren öffentlichen Schlüssel K_{B0} der autorisierten Instanz 60 und überträgt diesen zur Datenbank 20.

Schritt (14): Die Logik 70 sendet die Personenidentifikationsdaten (SID) der Standard-Instanz 101 verschlüsselt mit dem inneren öffentlichen Schlüssel K_{B0} der autorisierten Instanz 50 an die Datenbank 20.

Schritt (15): Die Logik 70 sendet die Personenidentifikationsdaten (BID) der autorisierten Instanz 50 verschlüsselt mit dem inneren öffentlichen Schlüssel K_{S0} der Standard-Instanz 101 an die Datenbank 20.

PATENTANSPRÜCHE

1. Datenverarbeitungssystem zur Verarbeitung von Objektdaten einer Vielzahl von Standard-Instanzen (101), wobei die Objektdaten Objektidentifikationsdaten (100) und zugehörige Nutzdaten (110) umfassen, mit einer Objektdaten-Datenbank (20), in welcher die Objektdaten über Zugriffseinrichtungen speicherbar und abrufbar sind, **dadurch gekennzeichnet**,

daß die Objektidentifikationsdaten (100) und die Nutzdaten (110) in der Objektdaten-Datenbank (20) voneinander getrennt speicherbar und abrufbar sind, sodaß allein aus den gespeicherten Datensätzen kein Zusammenhang zwischen den Objektidentifikationsdaten (100) und den Nutzdaten (110) ableitbar ist,

daß zumindest eine Eingabevorrichtung vorgesehen ist, welche bei Eingabe eines von für die Standard-Instanzen (101) vergebenen Sicherheitsschlüssel den Zugriff auf die Objektidentifikationsdaten (100) der zugeordneten Standard-Instanz und auf die zugehörigen Nutzdaten (110) ermöglicht,

daß gegebenenfalls für jede der Standard-Instanzen (101) zumindest eine zugeordnete Wiedergewinnungs-Instanz außerhalb der Objektdaten-Datenbank (20) definiert ist, über welche bei Verlust des Sicherheitsschlüssels dieser wieder erzeugt werden kann, und

daß der Sicherheitsschlüssel oder ein Teil davon bei der Standard-Instanz (101) und gegebenenfalls zusätzlich bei der zugeordneten Wiedergewinnungs-Instanz und/oder bei weiteren von der Standard-Instanz bestimmten Instanzen (50, 60) verbleibt oder von diesen auf ihn zugegriffen werden kann.

2. Datenverarbeitungssystem nach Anspruch 1, **dadurch gekennzeichnet**, daß mehrere voneinander unabhängige Systemoperator-Instanzen (30) vorhanden sind,

aus denen zwei oder mehrere Systemoperator-Instanzen für eine der Standard-Instanzen (101) als die dieser zugeordneten Wiedergewinnungs-Instanz definiert sind, ohne daß den ausgewählten Systemoperator-Instanzen die Identität der jeweils anderen ausgewählten Systemoperator-Instanz(en) sowie der Standard-Instanz(en) bekannt ist, wobei den zumindest zwei ausgewählten Systemoperator-Instanzen ein gemeinsamer Zugriff auf die Objektidentifikationsdaten in Verbindung mit den zugehörigen Nutzdaten für die jeweilige Standard-Instanz möglich ist.

3. Datenverarbeitungssystem nach Anspruch 1 oder 2, **dadurch gekennzeichnet**, daß weitere Instanzen (60, 50) definiert sind, welche durch die Standard-Instanzen (101) zum vollen oder teilweisen Datenzugriff autorisiert sind.

4. Datenverarbeitungssystem nach Anspruch 3, **dadurch gekennzeichnet**, daß die weiteren Instanzen eine oder mehrere assoziierte Instanzen (60) umfassen, die jeweils durch eine der Standard-Instanzen (101) autorisiert sind und die gleiche Zugriffsberechtigung wie diese aufweisen sowie weitere Instanzen autorisieren können.

5. Datenverarbeitungssystem nach Anspruch 4, **dadurch gekennzeichnet**, daß die assoziierten Instanzen (60) als Wiedergewinnungs-Instanzen definiert sind.

6. Datenverarbeitungssystem nach einem der Ansprüche 4 oder 5, **dadurch gekennzeichnet**, daß die weiteren Instanzen eine oder mehrere autorisierte Instanzen (50) umfassen, die jeweils durch eine der Standard-Instanzen (101) autorisiert sind, auf vorbestimmte Einträge in der Objektdaten-Datenbank (20) zuzugreifen.

7. Datenverarbeitungssystem nach Anspruch 4, 5 oder 6, **dadurch gekennzeichnet**, daß die weiteren Instanzen eine oder mehrere Forschungs-Instanzen (40) umfassen, die zum Zwecke der Analyse ausschließlich Zugriff auf die Nutzdaten (110) haben.

8. Datenverarbeitungssystem nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet**, daß jedem Eintrag mit Nutzdaten in der Objektdaten-Datenbank (20) eine Nutzdaten-Identifikation zugeordnet ist.

9. Datenverarbeitungssystem nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet**, daß der Sicherheitsschlüssel oder Teile davon auf einem Sicherheitstoken gespeichert ist, z.B. auf einer Smartcard (90), welche über einen PIN-Kode verfügt.

10. Datenverarbeitungssystem nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet**, daß die Objektdaten-Datenbank (20) durch zwei separate Datenbanken gebildet ist, wobei in der einen Datenbank Objektidentifikationsdaten und in der anderen Datenbank Nutzdaten gespeichert sind.

11. Datenverarbeitungssystem nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet**, daß die Objektdaten-Datenbank eine Personendaten-Datenbank ist und die Objektidentifikationsdaten (100) Personendaten, insbesondere Patientendaten sind.

12. Datenverarbeitungssystem nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet**, daß der Sicherheitsschlüssel jeder der Standard-Instanzen (101) aus einem oder mehreren inneren und einem oder mehreren äußeren Schlüssel gebildet ist, wobei die Verbindung der Nutzdaten mit den Objektidentifikationsdaten der jeweiligen Standard-Instanz dadurch erreicht wird, dass es einen innersten Schlüssel gibt, mit dem die Objektidentifikationsdaten verschlüsselt werden. Der äußere Schlüssel verbleibt jeweils bei den Standard-Instanzen (101) und bietet die Möglichkeit des Zugriffs auf den inneren Schlüssel. Der innere Schlüssel dient als Zugriffsmöglichkeit auf die innersten Schlüssel.

13. Verfahren zur Verarbeitung von Objektdaten von Standard-Instanzen, welche Objektidentifikationsdaten (100) und zugehörige Nutzdaten (110) umfassen, wobei in einem Speicherschritt die Objektdaten in einer Objektdaten-Datenbank (20)

gespeichert und in einem Abfrageschritt aus der Objektdaten-Datenbank auf die Objektdaten zugegriffen wird und diese abgerufen werden, **dadurch gekennzeichnet**,

daß im Speicherschritt die Objektidentifikationsdaten (100) und die Nutzdaten (110) in der Objektdaten-Datenbank (20) voneinander getrennt gespeichert werden, sodaß sie aus der Objektdaten-Datenbank (20) getrennt abgerufen werden können, allein aus den gespeicherten Datensätzen jedoch kein Zusammenhang zwischen den Objektidentifikationsdaten (100) und den Nutzdaten (110) ableitbar ist,

daß in einem Vergabeschritt Sicherheitsschlüssel an jede der Standard-Instanzen (101) vergeben werden, die ein Zugreifen auf die Objektidentifikationsdaten und die zugehörigen Nutzdaten für jede der Standard-Instanzen ermöglichen, wobei gegebenenfalls für jede der Standard-Instanzen eine Wiedergewinnungs-Instanz definiert wird, über welche bei Verlust des Sicherheitsschlüssels dieser wieder erzeugt werden kann,

daß jede der Standard-Instanzen weiteren Instanzen (60, 50) den vollen oder teilweisen Datenzugriff auf ihre Objektdaten gestatten kann,

und daß in einem Abfrageschritt über eine der Standard-Instanzen oder gegebenenfalls eine Wiedergewinnungs-Instanz und/oder eine der weiteren Instanzen (60, 50) nach Eingabe des Sicherheitsschlüssels oder eines Teils davon auf die Objektidentifikationsdaten (100) in Verbindung mit den zugehörigen Nutzdaten (110) zugegriffen wird.

14. Verfahren nach Anspruch 13, **dadurch gekennzeichnet**, daß für jede Standard-Instanz (101) zwei oder mehrere Systemoperator-Instanzen aus mehreren, voneinander unabhängigen Systemoperator-Instanzen (30) ausgewählt werden, ohne daß den ausgewählten Systemoperator-Instanzen die Identität der jeweils anderen ausgewählten Systemoperator-Instanz(en) bekannt ist, daß der Sicherheitsschlüssel der jeweiligen Standard-Instanz (101) auch an die zwei oder

mehreren, ausgewählten Systemoperator-Instanzen vergeben wird, sowie den zumindest zwei ausgewählten Systemoperator-Instanzen für den gemeinsamen Zugriff zur Verfügung steht,

und gegebenenfalls im Abfrageschritt über die zwei oder mehreren Systemoperator-Instanzen nach gemeinsamer Eingabe des Sicherheitsschlüssels auf die Objektidentifikationsdaten in Verbindung mit den zugehörigen Nutzdaten zugegriffen wird.

15. Verfahren nach Anspruch 13, **dadurch gekennzeichnet**, daß eine der weiteren Instanzen als Wiedergewinnungs-Instanz definiert ist, und bei Verlust des Sicherheitsschlüssels dieser über diese weitere Instanz erzeugt wird.

16. Verfahren nach Anspruch 14, **dadurch gekennzeichnet**, daß zur Erstellung des Sicherheitsschlüssels von einer Logik (70) für die Zuordnung von Objektidentifikationsdaten (100) und Nutzdaten (110) einer bestimmten Standard-Instanz (101) ein innerer Schlüssel der jeweiligen Standard-Instanz generiert wird und an diese Standard-Instanz (101) sowie an die zumindest zwei ausgewählten Systemoperator-Instanzen weitergeleitet wird, und daß der innere Schlüssel von dieser Standard-Instanz (101) und von den Systemoperator-Instanzen mit jeweils einem inneren Schlüssel verschlüsselt an die Objektdaten-Datenbank (20) zurückgesendet und dort abgelegt wird.

17. Verfahren nach Anspruch 16, **dadurch gekennzeichnet**, daß für die Eintragung von Nutzdaten (110) in der Objektdaten-Datenbank (20) ein weiterer Sicherheitsschlüssel generiert wird, der mit einem Sicherheitsschlüssel der Standard-Instanz und einem Sicherheitsschlüssel der ausgewählten Systemoperator-Instanzen verschlüsselt wird, wobei gegebenenfalls der weitere Sicherheitsschlüssel mit dem inneren Schlüssel der autorisierten und/oder assoziierten Instanz verschlüsselt wird.

Wien, am 21. November 2006

Braincon Handels-GmbH
durch:
HÄUPL & ELLMEYER KEG PATENTANWALTSKANZLEI

PATENTANWALTSKANZLEI
HÄUPL & ELLMEYER KEG
MARIAHILFERSTRASSE 50 (KIRCHENGASSE 1)
A-1070 WIEN
TEL. 523 16 01

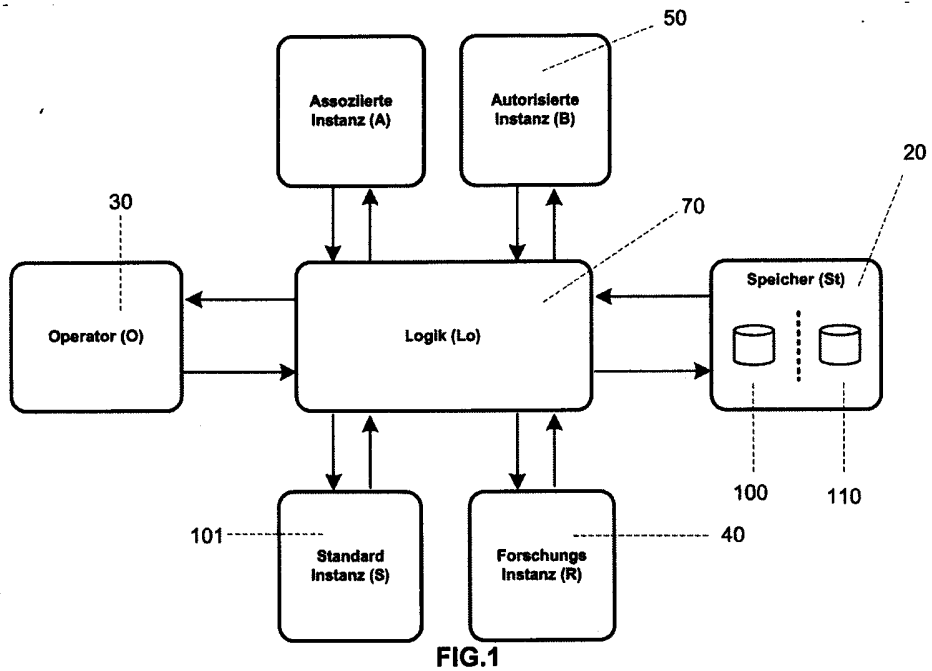

50
Assoziierte Instanz (A)
Autorisierte Instanz (B)
20
30
70
Speicher (St)
Operator (O)
Logik (Lo)
100
110
101
40
Standard Instanz (S)
Forschungs Instanz (R)

FIG.1

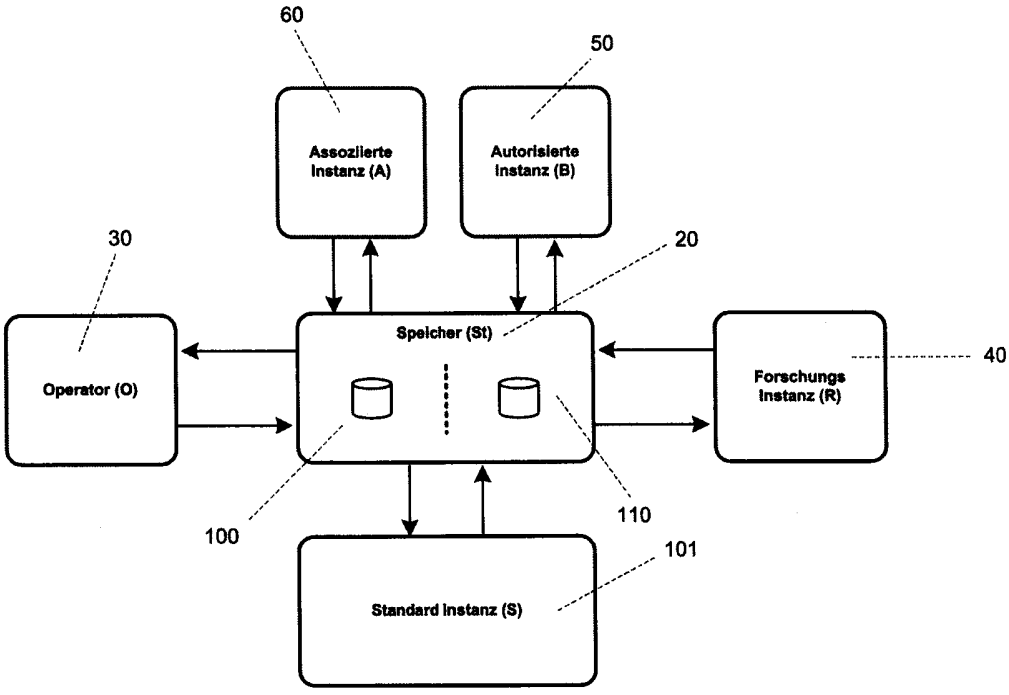

60
50
Assoziierte Instanz (A)
Autorisierte Instanz (B)
30
20
Speicher (St)
40
Operator (O)
Forschungs Instanz (R)
100
110
101
Standard Instanz (S)

FIG.2

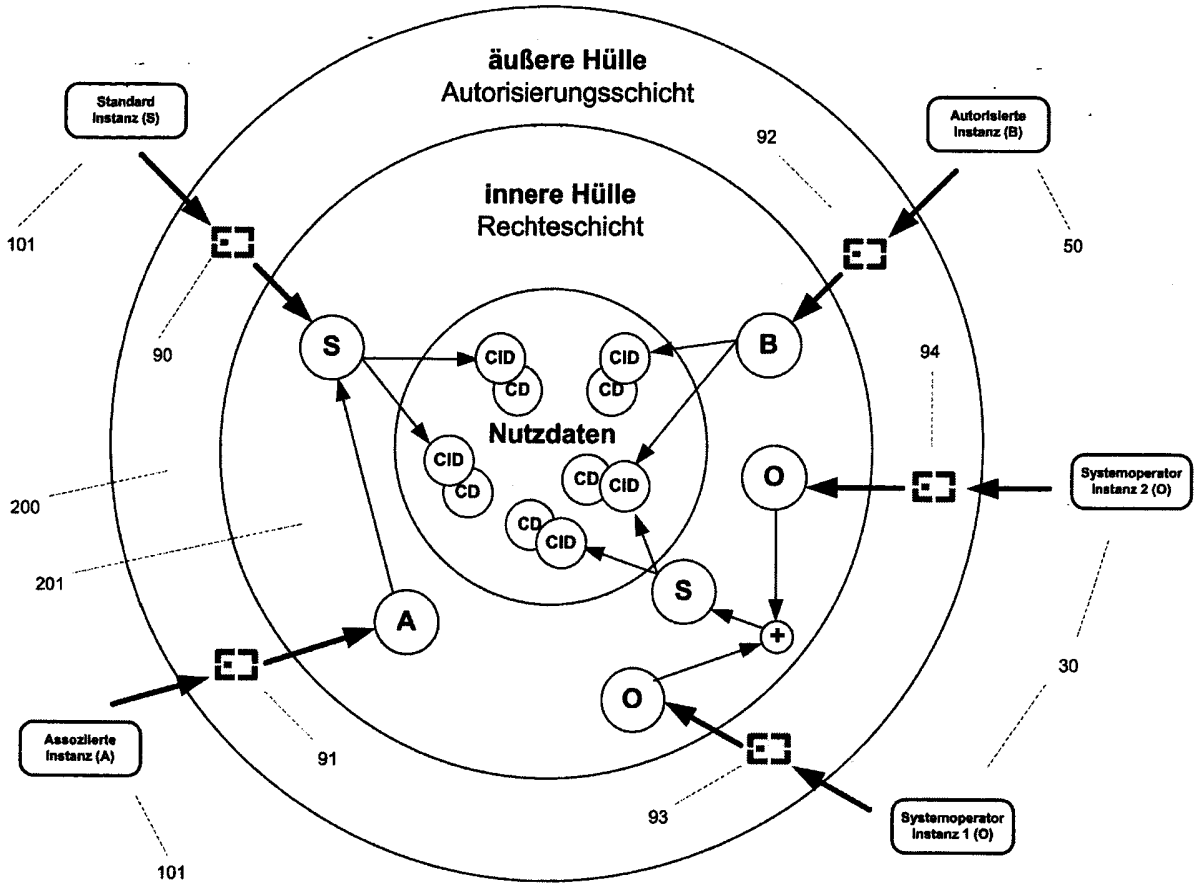

äußere Hülle
Autorisierungsschicht
innere Hülle
Rechteschicht
Nutzdaten
Standard Instanz (S)
Autorisierte Instanz (B)
Assoziierte Instanz (A)
Systemoperator Instanz 2 (O)
Systemoperator Instanz 1 (O)
S
B
A
O
CID
CD
101
90
92
50
94
200
201
30
91
93
101

FIG.3

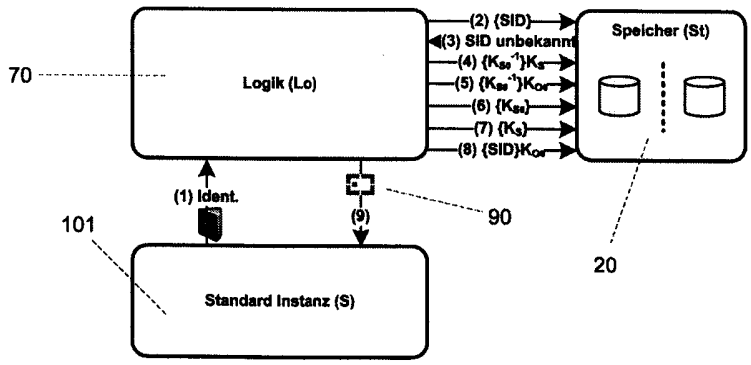

Logik (Lo)
Speicher (St)
Standard Instanz (S)
(1) Ident.
(2) {SID}
(3) SID unbekannt
(4) {Kso⁻¹}Ks
(5) {Kso⁻¹}Kor
(6) {Kso}
(7) {Ks}
(8) {SID}Kor
(9)
70
101
90
20

FIG.4

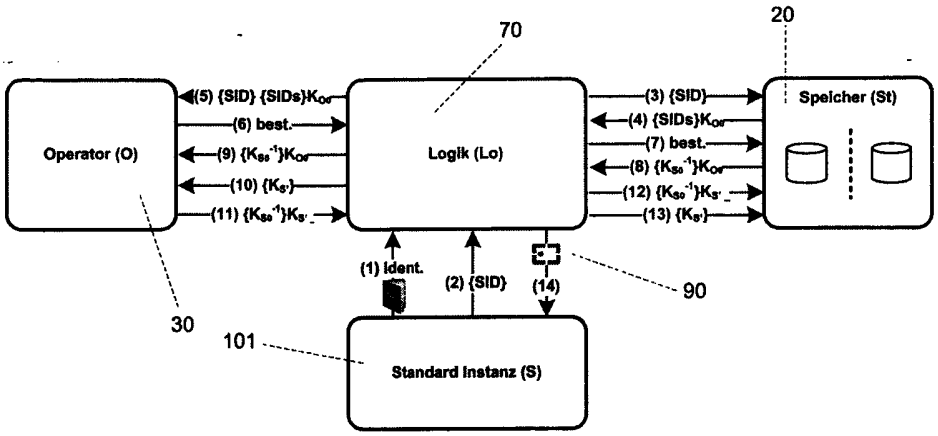


FIG.5

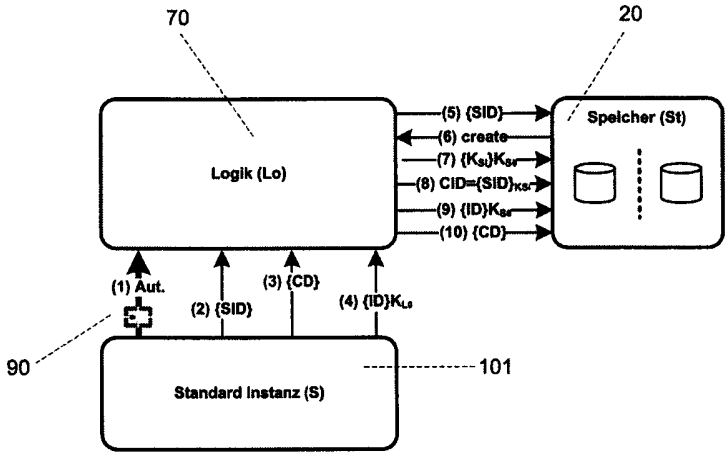


FIG.6

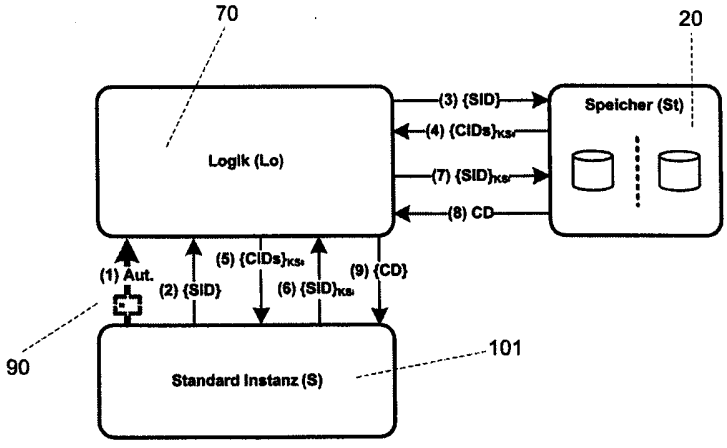


FIG.7

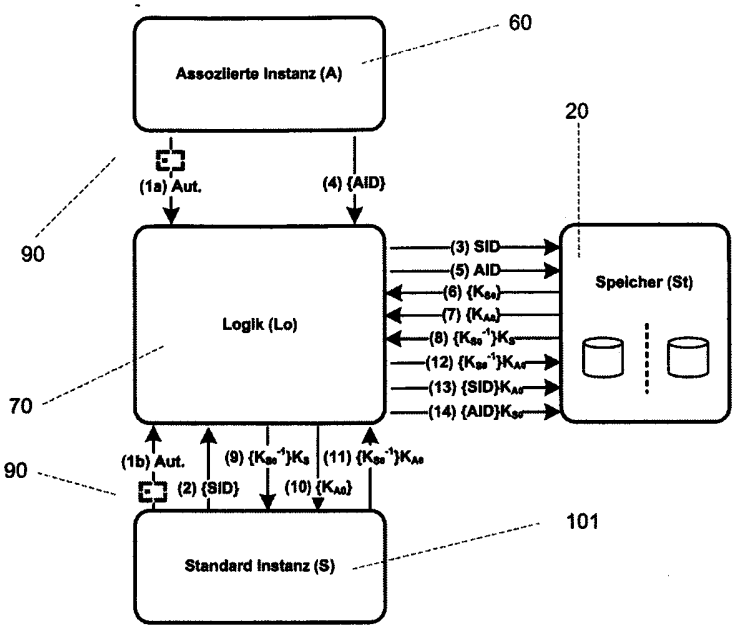

Assoziierte Instanz (A)
60
20
(1a) Aut.
(4) {AID}
90
Logik (Lo)
Speicher (St)
(3) SID
(5) AID
(6) {K_Sa}
(7) {K_AA}
(8) {K_Sa^-1}K_S
(12) {K_Sa^-1}K_AA'
(13) {SID}K_AA'
(14) {AID}K_Sa'
70
(1b) Aut.
(9) {K_Sa^-1}K_S
(11) {K_Sa^-1}K_AA
90
(2) {SID}
(10) {K_AA}
Standard Instanz (S)
101

FIG.8

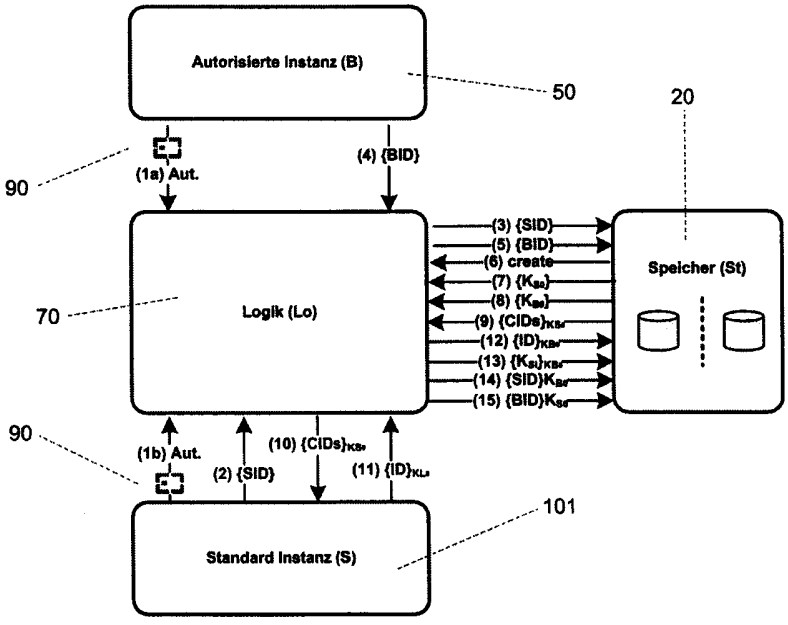

Autorisierte Instanz (B)
50
20
(4) {BID}
(1a) Aut.
90
Logik (Lo)
Speicher (St)
(3) {SID}
(5) {BID}
(6) create
(7) {K_Sa}
(8) {K_Sa}
(9) {CIDs}_KS'
(12) {ID}_KB'
(13) {K_S}_KB'
(14) {SID}K_Sa'
(15) {BID}K_Sa'
70
(1b) Aut.
(10) {CIDs}_KS'
(2) {SID}
(11) {ID}_KL'
90
Standard Instanz (S)
101

FIG.9

PATENTANWALTSKANZLEI
HÄUPL & ELLMEYER KEG
MARIAHILFERSTRASSE 50 (KIRCHENGASSE 1)
A-1070 WIEN TEL. 523 16 01

111495 - Braincon Handels-GmbH

A 1928/2006

Kl. G 06 F

NEUE PATENTANSPRÜCHE

1. Datenverarbeitungssystem zur Verarbeitung von Objektdaten einer Vielzahl von Standard-Instanzen (101), wobei die Objektdaten Objektidentifikationsdaten (100) und zugehörige Nutzdaten (110) umfassen, mit einer Objektdaten-Datenbank (20), in welcher die Objektdaten über Zugriffseinrichtungen speicherbar und abrufbar sind, **dadurch gekennzeichnet**,

daß die Objektidentifikationsdaten (100) und die Nutzdaten (110) in der Objektdaten-Datenbank (20) voneinander getrennt speicherbar und abrufbar sind, sodaß allein aus den gespeicherten Datensätzen kein Zusammenhang zwischen den Objektidentifikationsdaten (100) und den Nutzdaten (110) ableitbar ist,

daß zumindest eine Eingabevorrichtung vorgesehen ist, welche bei Eingabe eines von für die Standard-Instanzen (101) vergebenen Sicherheitsschlüssel den Zugriff auf die Objektidentifikationsdaten (100) der zugeordneten Standard-Instanz und auf die zugehörigen Nutzdaten (110) ermöglicht,

daß gegebenenfalls für jede der Standard-Instanzen (101) zumindest eine zugeordnete Wiedergewinnungs-Instanz außerhalb der Objektdaten-Datenbank (20) definiert ist, über welche bei Verlust des Sicherheitsschlüssels dieser wieder erzeugt werden kann, und

daß der Sicherheitsschlüssel oder ein Teil davon bei der Standard-Instanz (101) und gegebenenfalls zusätzlich bei der zugeordneten Wiedergewinnungs-Instanz und/oder bei weiteren von der Standard-Instanz bestimmten Instanzen (50, 60) verbleibt oder von diesen auf ihn zugegriffen werden kann.

2. Datenverarbeitungssystem nach Anspruch 1, **dadurch gekennzeichnet**, daß mehrere voneinander unabhängige Systemoperator-Instanzen (30) vorhanden sind, aus denen zwei oder mehrere Systemoperator-Instanzen für eine der Standard-Instanzen (101) als die dieser zugeordneten Wiedergewinnungs-Instanz definiert sind, ohne daß den ausgewählten Systemoperator-Instanzen die Identität der jeweils anderen ausgewählten Systemoperator-Instanz(en) sowie der Standard-Instanz(en) bekannt ist, wobei den zumindest zwei ausgewählten Systemoperator-Instanzen ein gemeinsamer Zugriff auf die Objektidentifikationsdaten in Verbindung mit den zugehörigen Nutzdaten für die jeweilige Standard-Instanz möglich ist.

3. Datenverarbeitungssystem nach Anspruch 1 oder 2, **dadurch gekennzeichnet**, daß weitere Instanzen (60, 50) definiert sind, welche durch die Standard-Instanzen (101) zum vollen oder teilweisen Datenzugriff autorisiert sind.

4. Datenverarbeitungssystem nach Anspruch 3, **dadurch gekennzeichnet**, daß die weiteren Instanzen eine oder mehrere assoziierte Instanzen (60) umfassen, die jeweils durch eine der Standard-Instanzen (101) autorisiert sind und die gleiche Zugriffsberechtigung wie diese aufweisen sowie weitere Instanzen autorisieren können.

5. Datenverarbeitungssystem nach Anspruch 4, **dadurch gekennzeichnet**, daß die assoziierten Instanzen (60) als Wiedergewinnungs-Instanzen definiert sind.

6. Datenverarbeitungssystem nach einem der Ansprüche 4 oder 5, **dadurch gekennzeichnet**, daß die weiteren Instanzen eine oder mehrere autorisierte Instanzen (50) umfassen, die jeweils durch eine der Standard-Instanzen (101) autorisiert sind, auf vorbestimmte Einträge, die der jeweiligen Standard-Instanz zugeordnet sind, z.B. bestimmte Patienten- oder Gesundheitsdaten, in der Objektdaten-Datenbank (20) zuzugreifen.

7. Datenverarbeitungssystem nach Anspruch 4, 5 oder 6, **dadurch gekennzeichnet**, daß die weiteren Instanzen eine oder mehrere Forschungs-Instanzen (40) umfassen, die zum Zwecke der Analyse ausschließlich Zugriff auf die Nutzdaten (110) haben.

8. Datenverarbeitungssystem nach einem Ansprüche 1 bis 7, **dadurch gekennzeichnet**, daß jedem Eintrag mit Nutzdaten in der Objektdaten-Datenbank (20) eine Nutzdaten-Identifikation zugeordnet ist.

9. Datenverarbeitungssystem nach einem der Ansprüche 1 bis 8, **dadurch gekennzeichnet**, daß der Sicherheitsschlüssel oder Teile davon auf einem Sicherheitstoken gespeichert ist, z.B. auf einer Smartcard (90), welche über einen PIN-Kode verfügt.

10. Datenverarbeitungssystem nach einem der Ansprüche 1 bis 9, **dadurch gekennzeichnet**, daß die Objektdaten-Datenbank (20) durch zwei separate Datenbanken gebildet ist, wobei in der einen Datenbank Objektidentifikationsdaten und in der anderen Datenbank Nutzdaten gespeichert sind.

11. Datenverarbeitungssystem nach einem der Ansprüche 1 bis 10, **dadurch gekennzeichnet**, daß die Objektdaten-Datenbank eine Personendaten-Datenbank ist und die Objektidentifikationsdaten (100) Personendaten, insbesondere Patientendaten sind.

12. Datenverarbeitungssystem nach einem der Ansprüche 1 bis 11, **dadurch gekennzeichnet**, daß der Sicherheitsschlüssel jeder der Standard-Instanzen (101) aus einem oder mehreren inneren und einem oder mehreren äußeren Schlüssel gebildet ist, wobei die Verbindung der Nutzdaten mit den Objektidentifikationsdaten der jeweiligen Standard-Instanz dadurch erreicht wird, dass es einen innersten Schlüssel gibt, mit dem die Objektidentifikationsdaten verschlüsselt werden, wobei der äußere Schlüssel jeweils bei den Standard-Instanzen (101) verbleibt und die

Möglichkeit des Zugriffs auf den inneren Schlüssel bietet, und wobei der innere Schlüssel als Zugriffsmöglichkeit auf die innersten Schlüssel dient.

13. Verfahren zur Verarbeitung von Objektdaten von Standard-Instanzen, welche Objektidentifikationsdaten (100) und zugehörige Nutzdaten (110) umfassen, wobei in einem Speicherschritt die Objektdaten in einer Objektdaten-Datenbank (20) gespeichert und in einem Abfrageschritt aus der Objektdaten-Datenbank auf die Objektdaten zugegriffen wird und diese abgerufen werden, **dadurch gekennzeichnet**,

daß im Speicherschritt die Objektidentifikationsdaten (100) und die Nutzdaten (110) in der Objektdaten-Datenbank (20) voneinander getrennt gespeichert werden, sodaß sie aus der Objektdaten-Datenbank (20) getrennt abgerufen werden können, allein aus den gespeicherten Datensätzen jedoch kein Zusammenhang zwischen den Objektidentifikationsdaten (100) und den Nutzdaten (110) ableitbar ist,

daß in einem Vergabeschritt Sicherheitsschlüssel an jede der Standard-Instanzen (101) vergeben werden, die ein Zugreifen auf die Objektidentifikationsdaten und die zugehörigen Nutzdaten für jede der Standard-Instanzen ermöglichen, wobei gegebenenfalls für jede der Standard-Instanzen eine Wiedergewinnungs-Instanz definiert wird, über welche bei Verlust des Sicherheitsschlüssels dieser wieder erzeugt werden kann,

daß jede der Standard-Instanzen weiteren Instanzen (60, 50) den vollen oder teilweisen Datenzugriff auf ihre Objektdaten gestatten kann,

und daß in einem Abfrageschritt über eine der Standard-Instanzen oder gegebenenfalls eine Wiedergewinnungs-Instanz und/oder eine der weiteren Instanzen (60, 50) nach Eingabe des Sicherheitsschlüssels oder eines Teils davon auf die Objektidentifikationsdaten (100) in Verbindung mit den zugehörigen Nutzdaten (110) zugegriffen wird.

14. Verfahren nach Anspruch 13, **dadurch gekennzeichnet**, daß für jede Standard-Instanz (101) zwei oder mehrere Systemoperator-Instanzen aus mehreren, voneinander unabhängigen Systemoperator-Instanzen (30) ausgewählt werden, ohne daß den ausgewählten Systemoperator-Instanzen die Identität der jeweils anderen ausgewählten Systemoperator-Instanz(en) bekannt ist, daß der Sicherheitsschlüssel der jeweiligen Standard-Instanz (101) auch an die zwei oder mehreren, ausgewählten Systemoperator-Instanzen vergeben wird, sowie den zumindest zwei ausgewählten Systemoperator-Instanzen für den gemeinsamen Zugriff zur Verfügung steht,

und gegebenenfalls im Abfrageschritt über die zwei oder mehreren Systemoperator-Instanzen nach gemeinsamer Eingabe des Sicherheitsschlüssels auf die Objektidentifikationsdaten in Verbindung mit den zugehörigen Nutzdaten zugegriffen wird.

15. Verfahren nach Anspruch 13, **dadurch gekennzeichnet**, daß eine der weiteren Instanzen als Wiedergewinnungs-Instanz definiert ist, und bei Verlust des Sicherheitsschlüssels dieser über diese weitere Instanz erzeugt wird.

16. Verfahren nach Anspruch 14, **dadurch gekennzeichnet**, daß zur Erstellung des Sicherheitsschlüssels von einer Logik (70) für die Zuordnung von Objektidentifikationsdaten (100) und Nutzdaten (110) einer bestimmten Standard-Instanz (101) ein innerer Schlüssel der jeweiligen Standard-Instanz generiert wird und an diese Standard-Instanz (101) sowie an die zumindest zwei ausgewählten Systemoperator-Instanzen weitergeleitet wird, und daß der innere Schlüssel von dieser Standard-Instanz (101) und von den Systemoperator-Instanzen mit jeweils einem inneren Schlüssel verschlüsselt an die Objektdaten-Datenbank (20) zurückgesendet und dort abgelegt wird.

17. Verfahren nach Anspruch 16, **dadurch gekennzeichnet**, daß für die Eintragung von Nutzdaten (110) in der Objektdaten-Datenbank (20) ein weiterer Sicherheitsschlüssel generiert wird, der mit einem Sicherheitsschlüssel der Standard-

Instanz und einem Sicherheitsschlüssel der ausgewählten Systemoperator-Instanzen verschlüsselt wird, wobei gegebenenfalls der weitere Sicherheitsschlüssel mit dem inneren Schlüssel der autorisierten und/oder assoziierten Instanz verschlüsselt wird.

Wien, am 10. Mai 2007

Braincon Handels-GmbH
durch:

HÄUPL & ELLMEYER KEG