(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 710 760 A1

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
11.10.2006 Patentblatt 2006/41

(51) Int Cl.:
G07F 19/00 *(2006.01)*

(21) Anmeldenummer: **05007519.1**

(22) Anmeldetag: **06.04.2005**

(84) Benannte Vertragsstaaten:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU MC NL PL PT RO SE SI SK TR
Benannte Erstreckungsstaaten:
AL BA HR LV MK YU

(71) Anmelder: **Scheidt & Bachmann GmbH**
41238 Mönchengladbach (DE)

(72) Erfinder:
- **Miller, Norbert**
  41063 Mönchengladbach (DE)
- **Busch, Erwin**
  41063 Mönchengladbach (DE)
- **Lowis, Josef**
  52525 Waldfeucht (DE)

(74) Vertreter: **Cohausz & Florack**
Patent- und Rechtsanwälte
Bleichstrasse 14
40211 Düsseldorf (DE)

Bemerkungen:
Geänderte Patentansprüche gemäss Regel 86 (2) EPÜ.

(54) Gesicherte Freigabe von Einrichtungen

(57) Die Erfindung betrifft ein Verfahren zur Freigabe zumindest einer Einrichtung bei dem die Freigabe zumindest teilweise durch mindestens einen ersten Code kontrolliert wird. Zur Einsparung von Personalkosten und zur Verbesserung der Sicherheit gegenüber ausspähen, wird vorgeschlagen, dass der erste Code mit Hilfe von Parametern von zumindest zwei Entitäten ermittelt wird.

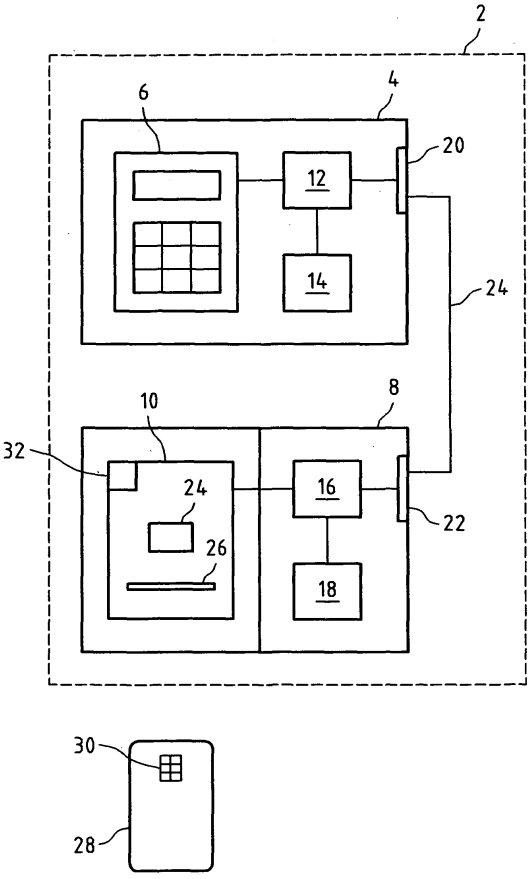

Fig.1

EP 1 710 760 A1

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zur Freigabe zumindest einer Einrichtung, bei dem die Freigabe zumindest teilweise durch mindestens einen ersten Code kontrolliert wird. Darüber hinaus betrifft die Erfindung eine Einrichtung sowie ein System zur Berechnung eines Freigabecodes. Außerdem betrifft die Erfindung ein Computerprogrammprodukt und ein Computerprogramm mit Instruktionen ausführbar auf einem Prozessor derart, dass zumindest eine Einrichtung freigegeben wird, wobei die Freigabe zumindest teilweise durch einen ersten Code kontrolliert wird.

[0002] Heutzutage ist es üblich, sicherheitsrelevante Einrichtungen mittels Codes vor einer Freigabe zu sichern. Solche Codes können beispielsweise persönliche Identifikationsnummern (PIN) sein. Die PIN können über ein Verschlüsselungsverfahren mit anderen Parametern verknüpft sein. Hierzu eignet sich beispielsweise das 3DES Verschlüsselungsverfahren, das auch in der Kreditwirtschaft eingesetzt wird. Bei diesem Verschlüsselungsverfahren wird mit Hilfe von zwei geheimen Schlüsseln in einem dreistufigen Verfahren der Parameter mit dem ersten Schlüssel verschlüsselt, mit dem zweiten Schlüssel entschlüsselt und schließlich mit dem zweiten Schlüssel verschlüsselt. Das Ergebnis ist eine PIN, die eindeutig mit dem Parameter verknüpft ist.

[0003] Zur Freigabe kann dann mit Hilfe der Parameter in der Einrichtung unter Nutzung der identischen, geheimen Schlüssel eine Vergleichs-PIN errechnet werden. Die Vergleichs-PIN wird mit der eingegebenen PIN verglichen. Bei Übereinstimmung kann eine Freigabe erfolgen.

[0004] Beispielsweise bei Geldautomaten in der Kreditwirtschaft, aber auch bei anderen benutzergesteuerten Automaten, bei denen die Benutzer selbsttätig sicherheitsrelevante Aktionen ausführen können, beispielsweise das Abheben von Geld, ist es notwendig, dass die hierfür erforderlichen geheimen Kundeninformationen von Dritten nicht abgehört werden können.

[0005] Bei der Abwicklung von Geldgeschäften werden Kunden aufgefordert, über eine Tastatur (PinPad) eine nur den Kunden bekannte geheime PIN einzugeben. Parallel wird von einer Kundenkarte mittels eines Kartenlesers eine Kundennummer oder eine Kontonummer ausgelesen, mit deren Hilfe die PIN erzeugt wurde. Für die Karteninhaberprüfung wird die PIN im Chip der Kundenkarte oder Online durch Rückfrage bei einer Zentrale auf Richtigkeit geprüft.

[0006] Dadurch, dass der Kartenleser unbemerkt aus der Frontwand des Geldautomaten ausgebaut werden und durch eine Attrappe ersetzt werden kann, ergeben sich für potentielle Angreifer Manipulationsmöglichkeiten. Insbesondere die Überprüfung der PIN in der Karte selber bietet aufgrund einer Übertragung der PIN auf die Karte im Klartext eine Angriffsmöglichkeit. Hier ist beispielsweise der so genannte "Kellen Angriff" bekannt geworden. Um diesen zu verhindern, ist vorgeschlagen worden, den Kartenleser über eine Sensorik mit dem Gehäuse des Geldautomaten zu verbinden. Die Sensorik bewirkt, dass, sobald der Kartenleser aus seiner Einbauposition von der Frontwand des Geldautomaten entfernt wird, alle sicherheitsrelevanten Daten im Kartenleser gelöscht werden. Dann ist der ausgebaute Kartenleser, auch wenn er im Gehäuse verbleibt, nicht mehr in der Lage, die vom PinPad verschlüsselt übertragene PIN zu entschlüsseln um eine Überprüfung der PIN in der Karte zu ermöglichen.

[0007] Um Kartenleser bei Ihrer Inbetriebnahme mit den sicherheitsrelevanten Daten zu speisen, wird das 4-Augen-Prinzip verfolgt. Dieses Prinzip beruht darauf, dass zwei Techniker vor Ort gemeinsam den Kartenleser und gegebenenfalls das PinPad einbauen und aktivieren. Die beiden Servicetechniker bauen den Kartenleser in die Frontwand ein und verbinden ihn mit dem PinPad. Um den Kartenleser zu aktivieren, müssen die sicherheitsrelevanten Daten in den Kartenleser eingespeist werden.

[0008] Hierzu wird gemäß des 4-Augen-Prinzips die PIN sowie die Personalnummer der beiden Servicetechniker abgefragt. Zunächst gibt ein erster Servicetechniker sein PIN und seine Personalnummer in das PinPad ein. Im PinPad kann mit Hilfe der Personalnummer eine Vergleichs-PIN errechnet werden und eine Teilfreigabe kann bei Übereinstimmung erfolgen. Der zweite Servicetechniker kann ebenfalls seine PIN und seine Personalnummer in das PinPad eingeben. Eine Überprüfung wird im PinPad durchgeführt. Für den Fall, dass beide PINs zu den eingegebenen Personalnummern gehören, kann eine Freigabe des PinPads erfolgen. Die sicherheitsrelevanten Daten können danach an den Kartenleser übertragen werden, um diesen zu aktivieren.

[0009] Durch die Eingabe sowohl des Pins als auch der Personalnummern von zwei Servicetechnikern ist gewährleistet, dass diese sich gegenseitig überwachen. Weiter wird im PinPad eine Protokolldatei geschrieben, in der die Daten der Servicetechniker, die die Freigabe bewirkt haben zusammen mit weiteren Daten gespeichert werden. Im Manipulationsfall kann im Nachhinein nachverfolgt werden, welche beiden Servicetechniker an der Aktivierung des Kartenlesers beteiligt waren.

[0010] Nachteilig an dem beschriebenen Verfahren ist jedoch, dass für die Installation jedes einzelnen Kartenlesers zwei Servicetechniker vor Ort sein müssen. Dies ist mit erheblichen Kosten verbunden. Auch kann nicht ausgeschlossen werden, dass die Personalnummer und die PIN eines Servicetechnikers von einem anderen Servicetechniker ausgespäht wird, beispielsweise bei der Eingabe in das PinPad. Im PinPad ist nicht überprüfbar, ob zwei unabhängige Personen Personalnummer und die entsprechende PIN eingegeben haben, oder ob diese Daten von nur einem Servicetechniker eingegeben wurden. Dies eröffnet eine Vielzahl von Manipulationsmöglichkeiten.

[0011] Es ist daher eine Aufgabe der Erfindung, ein Verfahren sowie eine Einrichtung und ein System zur Verfügung

zu stellen, welches eine kostengünstige Aktivierung von Einrichtungen ermöglicht. Eine weitere Aufgabe besteht darin, die Freigabe von Einrichtungen vor Manipulationen zu sichern.

[0012] Zur Lösung dieser Aufgabe schlägt die Erfindung ein Verfahren zur Freigabe zumindest einer Einrichtung vor, bei dem die Freigabe zumindest teilweise durch einen ersten Code kontrolliert wird, wobei der erste Code mit Hilfe von Parametern von zumindest zwei Entitäten ermittelt wird.

[0013] Einrichtungen können hierbei PinPads, Kartenleser, Geldautomaten, Ticketautomaten, Zugangsschranken, Schließfächer, Parkautomaten, Gleisanlagen oder sonstige technische Einrichtungen sein.

[0014] Die Freigabe einer solchen Einrichtung kann darin bestehen, dass Aktionen ausgelöst werden, Daten freigegeben oder übertragen werden.

[0015] Zur Freigabe der Einrichtung wird ein Code generiert, der von Parametern von zumindest zwei Entitäten ermittelt wird. Diese Parameter zusammen mit dem Code können in die Einrichtung eingegeben werden und dort überprüft werden. Ist der Code geeignet, die Einrichtung freizugeben, erfolgt die Freigabe.

[0016] Es ist ebenfalls bevorzugt, wenn zumindest zwei der Entitäten räumlich getrennt sind. Durch die räumliche Trennung der Entitäten und die Abhängigkeit des ersten Codes von den zwei Entitäten kann gewährleistet werden, dass die Freigabe der Einrichtung sicher ist. Es ist nicht möglich, dass beispielsweise eine Person vor Ort alleine den ersten Code erzeugt und somit die Einrichtung freigibt. Vielmehr müssen zwei räumlich getrennte Entitäten bei der Erzeugung des Codes eingebunden werden, was verhindert, dass eine Manipulation durch nur eine einzelne Person an der Einrichtung die Freigabe ermöglicht.

[0017] Es ist ebenfalls bevorzugt, dass mindestens eine Entität eine Person ist, und dass die von dieser Entität ermittelten Parameter personenbezogene Parameter sind. Hierbei ist es besonders bevorzugt, wenn der erste Code mit Parametern von zumindest zwei Personen erzeugt wird, die räumlich voneinander getrennt sind. Die personenbezogenen Parameter können beispielsweise Personaldaten, Personalnummern, Namen, Adressen, Geburtsdaten oder sonstige Parameter sein. Die personenbezogenen Parameter können von den Personen selbst angegeben werden.

[0018] Es ist ebenfalls bevorzugt, wenn mindestens eine Entität die freizugebende Einrichtung ist und wenn die von dieser Entität ermittelten Parameter einrichtungsbezogene Parameter sind. Einrichtungsbezogene Parameter können beispielsweise Stationsidentifikationen, Herstellerinformationen oder Stationsnamen sein. Die einrichtungsbezogenen Parameter lassen sich mit Hilfe der Einrichtung selbst ermitteln. Beispielsweise können diese an der Einrichtung abgelesen werden oder die Einrichtung gibt diese automatisch aus. Beispielsweise ist es möglich, dass die Einrichtung aus einem PinPad und einem Kartenleser gebildet ist. In diesem Fall können die einrichtungsbezogenen Parameter sowohl auf das PinPad als auch auf den Kartenleser bezogen sein. Beispielsweise können bei der Installation des Kartenlesers die auf den Kartenleser bezogenen Parameter vom Kartenleser auf das PinPad übertragen werden und von dem PinPad ausgegeben werden.

[0019] Besonders sicher lässt sich eine Freigabe gestalten, wenn gemäß eines vorteilhaften Ausführungsbeispiels die von einer Entität ermittelten Parameter zeitbezogene Parameter sind. Beispielsweise können die zeitbezogenen Parameter das aktuelle Datum, die aktuelle Uhrzeit, oder die Anzahl der Tage seit einem Stichtag sein. Mit den zeitbezogenen Parametern ist es möglich, dass der erste Code nur eine gewisse Gültigkeitsdauer hat. Beispielsweise kann ein zeitbezogener Parameter einen bestimmten Tag repräsentieren. Der Code, der mit diesem zeitbezogenen Parameter erzeugt wird, kann dann nur an diesem einen Tag eine Freigabe bewirken.

[0020] Es ist ebenfalls bevorzugt, wenn die von einer Entität ermittelten Parameter auftragsbezogene Parameter sind. Beispielsweise ist es möglich, dass Auftragsnummern erzeugt werden. Jedem einzelnen Freigabeauftrag kann somit eine eindeutige Nummer zugeordnet werden. Dadurch kann die Freigabe von Einrichtungen zurückverfolgt werden. Mit der Auftragsnummer kann nachvollzogen werden, mittels welcher Entitäten der Code erzeugt wurde und für welche Einrichtung dieser Code verwendet wurde. Dies ermöglicht eine Beweissicherung im Betrugsfall.

[0021] Zur Verwirklichung des 4-Augen-Prinzips wird auch vorgeschlagen, dass zumindest ein von einer einrichtungsseitigen Entität ermittelter Parameter an eine von der Einrichtung entfernte Zentrale übermittelt wird. Einrichtungsseitige Entitäten können beispielsweise die Einrichtung selbst, an die Einrichtung angeschlossene Vorrichtungen oder Personen die an der Einrichtung arbeiten sein. Mit Hilfe der einrichtungsseitigen Entität können Parameter ermittelt werden, die nur vor Ort unmittelbar an der Einrichtung feststellbar sind. Werden diese nur vor Ort feststellbaren Parameter an eine entfernte Zentrale übermittelt und dort zur Erzeugung eines Codes verwendet, wird gewährleistet, dass in der Zentrale kein Code erzeugt werden kann, der nicht unmittelbar für eine bestimmte Einrichtung bestimmt ist.

[0022] Es ist auch bevorzugt, wenn für die Berechnung des ersten Codes mindestens ein von einer zentralseitigen Entität ermittelter Parameter und mindestens ein von der einrichtungsseitigen Entität ermittelter Parameter verwendet wird. Die zentralseitige Entität kann dabei ein Techniker in der Zentrale oder auch eine beliebige Einrichtung in der Zentrale sein. Hierdurch wird gewährleistet, dass der erste Code sowohl von zentralseitigen als auch von einrichtungsseitigen Entitäten abhängig ist. Dies gewährleistet, dass nur durch ein Zusammenwirken der örtlich voneinander getrennten Entitäten der erste Code berechnet werden kann.

[0023] Zur Gewährleistung, dass in der Einrichtung der in der Zentrale errechnete erste Code überprüft werden kann und dass dieser erste Code abhängig von Parametern zentralseitiger Entitäten ist, wird der von der zentralseitigen Entität

ermittelte Parameter an die Einrichtung übermittelt. In diesem Fall kann die Freigabe nur unter Mithilfe von einrichtungsseitigen und zentralseitigen Entitäten erfolgen. Es ist nicht mehr möglich, dass sich beispielsweise zwei Servicetechniker bei der Eingabe von Personalnummer und PIN über die Schulter schauen und somit die PIN des jeweils anderen erspähen, um bei der Freigabe von weiteren Kartenlesern Manipulationen vornehmen zu können.

[0024] Um zu verhindern, dass der von der zentralseitigen Entität ermittelte Parameter im Klartext an eine einrichtungsseitige Entität übermittelt wird, wird vorgeschlagen, dass der mindestens eine von der zentralseitigen Entität ermittelte Parameter zumindest teilweise verschlüsselt wird. Dadurch wird verhindert, dass der Parameter von der zentralseitigen Entität im Klartext außerhalb der Zentral bekannt gemacht wird.

[0025] Um die Freischaltung mittels des zentralseitig berechneten ersten Codes zu bewirken, wird vorgeschlagen, dass der zentralseitig berechnete erste Code an die Einrichtung übermittelt wird. Hierbei ist es insbesondere vorteilhaft, wenn der zentralseitig berechnete erste Code zusammen mit den von der zentralseitigen Entität ermittelten Parametern in die Einrichtung eingegeben werden, um die Richtigkeit des ersten Codes überprüfen zu können.

[0026] Daher wird gemäß eines vorteilhaften Ausführungsbeispiels vorgeschlagen, dass der zentralseitig berechnete erste Code einrichtungsseitig zumindest mit Hilfe des mindestens einen von der Zentrale übermittelten zentralseitigen Parameters überprüft wird. Hierbei wird beispielsweise in die Einrichtung der erste Code zusammen mit den von der Zentrale übermittelten Parametern eingegeben. In der Einrichtung kann dann ein Vergleichscode berechnet und dieser mit dem ersten Code verglichen werden.

[0027] Um eine leichte Überprüfung des ersten Codes zu gewährleisten, wird vorgeschlagen, dass der erste Code zentralseitig und einrichtungsseitig mit derselben Rechenvorschrift berechnet wird. In der Zentrale wird mit Hilfe der Parameter von der zentralseitigen Entität und der Parameter von der einrichtungsseitigen Entität der erste Code berechnet. In der Einrichtung wird der erste Code zusammen mit den von der zentralseitigen Entität ermittelten Parametern und der einrichtungsseitigen Entität ermittelten Parametern eingegeben. In der Einrichtung kann ein Vergleichscode mit derselben Rechenvorschrift errechnet werden, um zu prüfen, ob der erste Code tatsächlich in der Zentrale mit denselben Informationen erstellt wurde. Stimmen erster Code und Vergleichscode überein, kann eine Freigabe zumindest teilweise erfolgen.

[0028] Weiter ist es bevorzugt, dass zumindest der erste Code mittels eines symmetrischen Verschlüsselungsverfahren berechnet wird. Hierbei kann beispielsweise ein DES Verschlüsselungsverfahren zum Einsatz kommen. Auch ist es möglich, ein 3DES Verschlüsselungsverfahren einzusetzen. Die Verschlüsselungsverfahren können Schlüssellängen von 56 Bit bzw. 112 Bit aufweisen. Ferner sind Verschlüsselungsverfahren nach dem CAST-128 Algorithmus, dem Twofish-Algorithmus, dem Blowfish-Algorithmus und dem asymmetrischen IDEA-Algorithmus möglich.

[0029] Um zu gewährleisten, dass die Freigabe nur dann erfolgt, wenn zwei voneinander unabhängige Codes vorhanden sind, wird vorgeschlagen, dass die Freigabe der Einrichtung zumindest durch den ersten Code und einen zweiten Code kontrolliert wird. Beispielsweise kann der zweite Code ein von einer einrichtungsseitigen Entität eingegebener PIN sowie ein entsprechender Parameter der einrichtungsseitigen Entität sein. Es versteht sich, dass der zweite Code als weitere Sicherung gegenüber Manipulationsversuchen dient. Eine Freigabe kann jedoch mit nur dem ersten Code erfolgen, wenn dies so festgelegt wurde.

[0030] Besonders bevorzugt ist es, wenn der zweite Code mit Hilfe von personenbezogenen Parametern ermittelt wird. Hierbei kann beispielsweise mit Hilfe einer Personalnummer ein PIN als zweiter Code erzeugt werden. Der zweite Code kann zusammen mit den personenbezogenen Parametern in die Einrichtung eingegeben werden. In der Einrichtung kann ein Vergleichscode mit Hilfe der personenbezogenen Parameter errechnet werden, der mit dem eingegebenen zweiten Code verglichen wird.

[0031] Durch die Bezeichnung der Codes als erster Code und zweiter Code ist deren Reihenfolge nicht festgelegt. Vielmehr ist für eine Freigabe die Reihenfolge der beiden Codes beliebig. Auch können neben dem ersten und dem zweiten Code noch weitere Codes zur Freigabe notwendig sein.

[0032] Um zu verhindern, dass der zentralseitig berechnete erste Code anderen Entitäten als der Einrichtung selbst bekannt gemacht wird, wird vorgeschlagen, dass der erste Code über eine direkte elektronische Kommunikationsverbindung zwischen der Einrichtung und der Zentrale übermittelt wird. Die elektronische Kommunikationsverbindung kann dabei drahtgebunden oder drahtlos, paketvermittelt oder leitungsvermittelt sein. Die Übertragung kann dabei beispielsweise über Mobilfunk, Wireless-LAN, Internet, ISDN oder DSL erfolgen. Der erste Code kann unmittelbar von der Zentrale an die Einrichtung übermittelt werden, ohne dass beispielsweise ein Servicetechniker vor Ort in die Übertragung verwickelt ist.

[0033] Der Servicetechniker vor Ort könnte die Generierung des ersten Codes in der Zentrale durch die Eingabe seines personenbezogenen Codes zusammen mit seinen personenbezogenen Daten auslösen. Nach der Eingabe seines personenbezogenen Codes mit seinen personenbezogenen Parametern kann die Einrichtung den personenbezogenen Code überprüfen. Ist die Überprüfung korrekt, kann die Zentrale automatisch von der Einrichtung dazu aufgefordert werden, den ersten Code zu erzeugen, indem beispielsweise die personenbezogenen Parameter des Servicetechnikers vor Ort und einrichtungsbezogene Parameter an die Zentrale übermittelt werden. In der Zentrale kann dann der erste Code mit den personenbezogenen Parametern des Servicetechnikers vor Ort, den einrichtungsbezogenen

Parametern und zentralseitigen Parametern erzeugt und zurück an die Einrichtung übermittelt werden. Zu den zentralseitigen Parametern können beispielsweise auch eine Personalnummer und ein PIN eines Mitarbeiters in der Zentrale gehören. Zusammen mit der Übermittlung des ersten Codes werden die Parameter, die zur Erzeugung des ersten Codes verwendet wurden, übermittelt. Die Einrichtung wird in die Lage versetzt, einen Vergleichscode zu erzeugen, der mit dem ersten Code verglichen werden kann. Bei einer Übereinstimmung kann dann die vollständige Freigabe erfolgen.

[0034] Ein weiterer Gegenstand der Erfindung ist eine Einrichtung umfassend Eingabemittel zur Eingabe von Parametern von zumindest zwei Entitäten und zur Eingabe mindestens eines ersten Codes, und Freigabemittel zur zumindest teilweisen Freigabe der Einrichtung bei positiver Überprüfung zumindest des ersten mit Hilfe von Parametern von zumindest zwei Entitäten ermittelten Codes.

[0035] Ein zusätzlicher Gegenstand der Erfindung ist ein System zur Berechung eines Freigabecodes, mit einer zuvor beschriebenen Einrichtung und einer Zentrale, dadurch gekennzeichnet, dass die Zentrale zur Berechnung zumindest eines ersten Codes mit Hilfe von Parametern von zumindest zwei Entitäten eingerichtet ist.

[0036] Ein weiterer Aspekt der Erfindung betrifft ein Computerprogrammprodukt sowie ein Computerprogramm mit Instruktionen ausführbar auf einem Prozessor derart, dass zumindest eine Einrichtung freigegeben wird, wobei die Freigabe zumindest teilweise durch mindestens einen ersten Code kontrolliert wird und der erste Code mit Hilfe von Parametern von zumindest zwei Entitäten ermittelt wird.

[0037] Weitere Vorteile ergeben sich aus den nachgeordneten Ansprüchen.

[0038] Die Erfindung wird nachfolgend anhand einer Ausführungsbeispiele zeigenden Zeichnung näher erläutert. In der Zeichnung zeigen:

Fig. 1 einen Verkaufsautomaten mit einem PinPad und einem Kartenleser;

Fig. 2 ein System mit einem Verkaufsautomaten und einer davon entfernten Zentrale;

Fig. 3 ein Ablaufdiagramm eines erfindungsgemäßen Verfahrens.

[0039] Fig. 1 zeigt einen Verkaufsautomaten 2 mit einem in einem Gehäuse 4 untergebrachten PinPad 6 und in einem Gehäuse 8 untergebrachten Kartenleser 10. Der Verkaufsautomat 2 kann beispielsweise ein Ticketautomat oder ein Geldautomat sein.

[0040] Neben dem PinPad 6 sind in dem Gehäuse 4 ein Mikroprozessor 12 und ein Speicherbereich 14 angeordnet. Das Gehäuse 4 ist ein "temper responsive" Gehäuse, was bedeutet, dass das Gehäuse 4 nicht zerstörungsfrei geöffnet werden kann. Beim Öffnen des Gehäuses 4 gehen alle im Mikroprozessor 12 und Speicherbereich 14 gespeicherten Daten verloren.

[0041] Weiterhin sind im Verkaufsautomat 2 in dem Gehäuse 8 ein Kartenleser 10, ein Mikroprozessor 16 und ein Speicherbereich 18 angeordnet. Das Gehäuse 8 ist ebenfalls ein "temper responsive" Gehäuse.

[0042] Eine Kommunikation zwischen dem Mikroprozessor 12 und dem Mikroprozessor 16 innerhalb des Verkaufsautomaten 2, außerhalb der Gehäuse 4, 8 erfolgt über Schnittstellen 20, 22 und Datenleitung 24. Die Schnittstellen können herkömmliche Kommunikationsschnittstellen sein, beispielsweise Firewire (IEEE1394), RS232 oder USB.

[0043] Der Kartenleser 10 weist eine Chip-Kontaktiereinheit 24 und einen Kartenschlitz 26 auf. Das Gehäuse 8 ist so gestaltet, dass in den Verkaufsautomaten 2 in einer Frontblende lediglich der Kartenleser 10 zu sehen ist und der Mikroprozessor 16 und der Speicherbereich 18 unsichtbar im Inneren des Verkaufsautomaten 2 angeordnet sind.

[0044] Im Regelfall, nachdem der Kartenleser 10 aktiviert wurde, kann ein Kunde mit einer Chipkarte 28 den Verkaufsautomaten 2 betätigen. Hierzu wird die Chipkarte 28 in den Kartenschlitz 26 eingeführt und die Chipkontakte des Chips 30 mit Hilfe der Chip-Kontaktiereinheit 24 kontaktiert. Über die Chipkontakte des Chips 30 können Kundendaten, beispielsweise eine Kontonummer, ausgelesen werden.

[0045] Die ausgelesene Kontonummer kann über den Mikroprozessor 16, die Schnittstelle 22, die Datenleitung 24 und die Schnittstelle 20 an den Mikroprozessor 12 übertragen werden.

[0046] Der Kunde kann das PinPad 6 dazu verwenden, seine persönliche PIN einzugeben. Im Falle einer Online-Überprüfung der Gültigkeit der PIN wird diese nach der Eingabe mit Hilfe des Mikroprozessors 16 und zumindest eines in dem Speicherbereich 14 gespeicherten geheimen Schlüssels verschlüsselt und über einen Netzbetreiberrechner zu einer Autorisierungsstelle gesendet. Die Autorisierungsstelle kann Online die PIN mit Hilfe der Kontonummer auf Richtigkeit überprüfen und die vom Kunden am Verkaufsautomaten 2 gewünschte Aktion ebenfalls über den Netzbetreiberrechner bewirken.

[0047] Eine Offline-PIN-Überprüfung kann in dem Chip 30 der Chipkarte 28 erfolgen. Hierzu wird die von einem Kunden in das PinPad 6 eingegebene PIN über den Mikroprozessor 12, die Schnittstelle 20, die Datenleitung 24 und die Schnittstelle 22 an den Mikroprozessor 16 übertragen. Da die PIN außerhalb der Gehäuse 4, 8 übertragen wird, und somit nicht mehr innerhalb der "temper responsive" Bereiche ist, wird die in das PinPad 6 eingegebene PIN im Mikroprozessor 12 verschlüsselt und nach der Übertragung über die Datenleitung 24 im Mikroprozessor 16 entschlüsselt. Für

die Ver- und Entschlüsselung der PIN in den Mikroprozessoren 12, 16 sind geheime Schlüssel in den Speicherbereichen 14, 18 abgespeichert.

[0048] Die entschlüsselte PIN wird über die Chip-Kontaktiereinheit 24 unmittelbar an die Chipkontakte des Chips 30 angelegt. Hierbei liegt die PIN an den Chipkontakten des Chips 30 unverschlüsselt an. Im Chip 30 wird eine Überprüfung der PIN durchgeführt und im Falle einer positiven Überprüfung wird über den Mikroprozessor 16 eine vom Kunden am Verkaufsautomaten 2 gewünschte Aktion bewirkt.

[0049] Die Offline-Überprüfung der PIN birgt jedoch Manipulationsrisiken. Wie bereits erwähnt, ist lediglich der Kartenleser 10 in der Frontwand des Verkaufsautomaten 2 zu erkennen. Es besteht nun die Möglichkeit, den Kartenleser 10 von der Frontwand des Gehäuses 2 zu entfernen und eine Attrappe eines Kartenlesers in der Frontwand des Verkaufsautomaten 2 einzubauen. Diese Attrappe verfügt ebenfalls über eine Chip-Kontaktiereinheit. Die Chip-Kontaktiereinheit der Attrappe ist mit der Chip-Kontaktiereinheit 24 des ausgebauten Kartenlesers 10 verbunden. Der Kartenleser 10 kann im Inneren des Gehäuses 2 versteckt sein. Im Falle der Offline-PIN-Überprüfung wird, wie vorher erwähnt, über den Mikroprozessor 16 die in das PinPad 6 eingegebene PIN an den Kartenleser 10 übertragen. An der Chip-Kontaktiereinheit 24 des Kartenlesers 10, der sich im Inneren des Verkaufsautomaten 2 befindet, liegt die PIN im Klartext an. Über eine Datenleitung ist die Chip-Kontaktiereinheit 24 mit der Chip-Kontaktiereinheit der Attrappe in der Frontwand des Verkaufsautomaten 2 verbunden. Die PIN-Überprüfung im Chip 30 erfolgt, ohne dass der Kunde etwas bemerkt. Jedoch kann auf der Datenleitung zwischen der Chip-Kontaktiereinheit 24 und der Chip-Kontaktiereinheit der Attrappe die PIN im Klartext abgegriffen werden. Geschieht dies, kann der Angreifer ohne weiteres in Zukunft die PIN verwenden, um eventuell mit einer manipulierten Karte an einem anderen Verkaufsautomaten einen Zahlungsvorgang auszulösen.

[0050] Die oben beschriebene Manipulationsmöglichkeit besteht daher, weil der Kartenleser 10, ohne seine Funktionalität zu verlieren, aus der Frontwand des Verkaufsautomaten 2 ausgebaut und durch eine Attrappe ersetzt werden kann. Um einen solchen Missbrauch zu verhindern, wird der Kartenleser 10 mit einer Sensorik 32 versehen, die den Ausbau des Kartenlesers 10 aus der Frontwand des Verkaufsautomaten 2 detektiert. In diesem Fall werden alle auf dem Mikroprozessor 16 und im Speicherbereich 18 gespeicherten Daten gelöscht. Dadurch, dass die Daten im Mikroprozessor 16 und im Speicherbereich 18 gelöscht wurden, kann eine vom Mikroprozessor 12 verschlüsselt übertragene PIN im Mikroprozessor 16 nicht mehr entschlüsselt werden und eine Klartextübertragung der PIN an die Chip-Kontaktiereinheit 24 wird unmöglich.

[0051] Für eine Wiederinbetriebnahme des Kartenlesers 10 oder für einen Neueinbau eines Kartenlesers 10 muss dieser aktiviert werden. Bei der Aktivierung müssen die geheimen Informationen, insbesondere die Schlüssel für die Entschlüsselung der auf der Datenleitung 24 verschlüsselt übertragenen PIN vom PinPad 6 in den Kartenleser 10 geladen werden.

[0052] Hierzu wird das 4-Augen-Prinzip eingesetzt. Ein Servicetechniker vor Ort wird, nachdem er den Kartenleser 10 in die Frontwand des Verkaufsautomaten 2 eingebaut hat, aufgefordert, seine persönliche PIN und seine Personalnummer in das PinPad 6 einzugeben. Mit Hilfe der Personalnummer wird im Mikroprozessor 12 unter Verwendung zumindest eines geheimen Schlüssels eine Vergleichs-PIN errechnet und diese mit der vom Servicetechniker eingegebenen PIN verglichen. Stimmen diese beiden überein, hat der Servicetechniker die korrekte, seiner Personalnummer zugehörige PIN eingegeben.

[0053] Danach wird ein zweiter Servicetechniker vor Ort aufgefordert, seine PIN und seine Personalnummer in das PinPad 6 einzugeben. Diese zweite PIN wird gleichfalls mit Hilfe des Mikroprozessors 12 überprüft. Sind beide PIN mit den entsprechenden Personalnummern verknüpft, werden über die Schnittstelle 20, die Datenleitung 24 und die Schnittstelle 22 alle sicherheitsrelevanten Schlüssel vom PinPad 6 in den Kartenleser 10 geladen. Bei dieser Übertragung werden die Daten verschlüsselt, um einen Abgriff auf der Datenleitung 24 zu verhindern. Nach der Übertragung der Schlüssel werden diese im Speicherbereich 18 des Kartenlesers 10 gespeichert und können fortan für die Entschlüsselung von verschlüsselten PIN verwendet werden. Der Kartenleser eignet sich nun wieder für die Offline-Überprüfung von PIN.

[0054] Nachteilig bei dem beschriebenen Verfahren ist jedoch, dass zwei Servicetechniker vor Ort anwesend sein müssen, um einen Kartenleser 10 zu aktivieren. Dies ist mit hohen Kosten verbunden. Außerdem ist es möglich, dass sich die Servicetechniker ausspähen und die PIN und Personalnummer des jeweils anderen Servicetechnikers erspähen. Dann wäre es möglich, dass ein einzelner Servicetechniker vor Ort eine Aktivierung eines Kartenlesers 10 bewirkt.

[0055] Erfindungsgemäß ist ein Verfahren entwickelt worden, welches es erlaubt, den Austausch und die Aktivierung des Kartenlesers vor Ort mit nur einem Servicetechniker durchzuführen, wobei jedoch dass 4-Augen-Prinzip gewahrt bleibt.

[0056] Fig. 2 zeigt ein System zur Durchführung des erfindungsgemäßen Verfahrens. Ein Servicetechniker 34 kann die Aktivierung eines Kartenlesers 10 in einem Verkaufsautomaten 2 vor Ort betreuen. Der Servicetechniker 34 bzw. der Verkaufsautomat 2 ist über eine Kommunikationsverbindung 36 mit einem Kommunikationsnetz 38 verbunden. Die Kommunikationsverbindung 36 kann dabei beispielsweise eine Mobilfunkverbindung sein. Über das Kommunikationsnetz 38 wird eine Kommunikationsverbindung 40 mit einer Zentrale 42 hergestellt. In der Zentrale 42 kann ein Servicetechniker 44 die Aktivierung des Kartenlesers für Verkaufsautomaten 2 begleiten. Eine bidirektionale Datenkommuni-

kation zwischen Zentrale 42 und Servicetechniker 44 sowie Verkaufsautomat 2 und Servicetechniker 34 ist über die Kommunikationsverbindung 36, das Kommunikationsnetz 38 und die Kommunikationsverbindung 40 gewährleistet.

[0057] Fig. 3 zeigt ein Ablaufdiagramm eines erfindungsgemäßen Verfahrens. Zunächst fährt ein Servicetechniker 34 zu einem Verkaufsautomaten 2 um einen Kartenleser 10 zu aktiven.

[0058] Nach dem Einbau des Kartenlesers 10 in den Verkaufsautomaten 2 meldet sich dieser Kartenleser 10 über die Datenleitung 24 bei dem PinPad 6 an. Bei der Anmeldung kann der Kartenleser 10 beispielsweise seine Terminalidentifikation (TID), seine Stationsnummer (STAT_ID) und seine Stations-Issuer-Nummer (STAT_ISS) an das PinPad 6 übermitteln. Darüber können an das PinPad 6 eine weitere Kennung (S&B_ID) sowie eine Konstante (K1) übermittelt werden. Diese Informationen sind einrichtungsseitige Parameter. Die einrichtungsseitigen Parameter werden von dem Kartenleser 10 bzw. dem Verkaufsautomaten 2 an das PinPad 6 übertragen (50).

[0059] Das PinPad 6 meldet (52) dem Servicetechniker 34, dass der Kartenleser aktiviert werden muss. Es ist auch denkbar, dass der Servicetechniker 34 unmittelbar am PinPad 6 durch Eingabe einer Tastenkombination eine Aktivierung eines Kartenlesers 10 beginnt.

[0060] Für die Aktivierung des Kartenlesers 10 gibt der Servicetechniker 34 seine persönliche Identifikationsnummer (PIN_ST) sowie seine Personalnummer (PNR_ST) in das PinPad 6 ein (54). Im PinPad 6 wird im Mikroprozessor 12 die eingegebene PIN_ST überprüft. Hierzu wird in dem Mikroprozessor 12 die Operation

$$PIN\_ST = ((3DES_e \quad K_{SB\_Key}(PNR\_ST \mid S\&B\_ID \mid K1) \; MOD \; 0xF00000) \; MOD \; 1000000)$$

durchgeführt. Beim oben verwendeten $3DES_e$ K_{SB_Key} (x) Verfahren werden die Parameter x in einem dreistufigen DES Verfahren mit zwei geheimen Schlüsseln K_{SB_Key} verschlüsselt. Die PIN_ST die der Servicetechniker eingegeben hat, ist bereits zuvor mit selbigen Parametern und der gleichen Rechenvorschrift ermittelt worden. Stimmt die eingegebene PIN_ST mit der errechneten überein, ist ein erster Schritt einer Freigabe eines Kartenlesers 10 erfolgt.

[0061] Das PinPad 6 meldet dem Servicetechniker 34 die erfolgreiche Teilfreigabe (56) 56. Darüber hinaus zeigt das PinPad 6 dem Servicetechniker 34 einrichtungsbezogene Parameter wie beispielsweise TID, STAT_ID, STAT_ISS, DAT, K1 an.

[0062] Der Servicetechniker 34 übermittelt (58) die einrichtungsbezogenen Parameter zusammen mit seiner eigenen Personalnummer (PNR_ST) über eine Kommunikationsverbindung an die Zentrale 42. Weiter übermittelt der Servicetechniker einen Zeitstempel DAT an die Zentrale. Der Zeitstempel kann den aktuellen Tag repräsentieren und ermöglicht die Begrenzung der Freigabe auf einen bestimmten Tag.

[0063] Die Zentrale 42 fordert den Servicetechniker 44 in der Zentrale auf (60), seine Personalnummer (PNR_RM) und/oder seine PIN (PIN_RM) bekannt zu geben. Der Servicetechniker 44 übermittelt (62) seine Personalnummer und/oder seine PIN an einen Rechner in der Zentrale 42.

[0064] Nach Überprüfung der Personalnummer (PNR_RM) und der PIN (PIN_RM) in der Zentrale 42, beispielsweise ebenfalls mittels 3DES, wird die Generierung eines Auftrags freigegeben. Die Erzeugung eines neuen Auftrags muss erneut mit PIN und PNR_RM freigegeben werden.

[0065] Zunächst wird in der Zentrale die Personalnummer des Servicetechnikers 44 verschlüsselt. Hierzu wird die Personalnummer des Servicetechnikers 44 (PNR_RM), die Terminalnummer (TID), eine zweite Konstante (K2), die weitere Kennung (S&B_ID) und das aktuelle Datum (DAT) verwendet. Das aktuelle Datum (DAT) kann auch mittels einer Anzahl von Tagen seit einem Stichtag errechnet worden sein. In der Zentrale 42 wird eine codierte Personalnummer (PNR_RM*) mittels einer Verschlüsselung gemäß

$$PNR\_RM^{*} = (((3DES_{e}\ K_{SB\_Key}(\ PNR\_RM\ |\ S\&B\_ID\ |\ TID\ |\ DAT\ |\ K2)\ MOD\ 0xF000)\ MOD\ 1000$$

erzeugt. Die verschlüsselte Personalnummer PNR_RM* wird auf 3 Dezimalstellen mittels MOD 0xF000 und MOD 1000 trunkiert.

[0066] Nachdem die verschlüsselte Personalnummer PNR_RM* erzeugt wurde, wird in der Zentrale 42 eine eindeutige Auftragsnummer (AUFT_ID) erzeugt. Mit Hilfe der Auftragsnummer (AUFT_ID), der verschlüsselten Personalnummer (PNR_RM*), des Datums (DAT) und weiteren Parametern wird eine verschlüsselte Auftragsnummer (AUFTRAG*) mittels

$$AUFTRAG^{*} = ((3DES_{e}\ K_{SB\_Key}(AUFT\_ID\ |\ PNR\_RM^{*}\ |\ S\&B\_ID\ |\ DAT)\ MOD\ 0xF00)$$

errechnet. Die verschlüsselte Auftragsnummer wird auf zwei Dezimalstellen mittels MOD 0xF00 trunkiert.

[0067] Schließlich wird in der Zentrale 42 eine PIN (PIN_AT) mittels

$$PIN\_AT = (((3DES_{e}\ K_{SB\_Key}(\ PNR\_ST\ |\ AUFTRAG*\ |\ TID\ |\ STAT\_ID\ |\ STAT\_ISS)\ MOD\ 0xF00000)\ MOD\ 1000000)\ \&\ 0xFFF000)\ +\ PNR\_RM^{*})$$

berechnet. Die PIN_AT enthält einen verschlüsselten 6-stelligen Dezimalwert, der mittels 3-DES aus Personalnummer des Servicetechnikers vor Ort (PNR_ST), der verschlüsselten Auftragsnummer (AUFTRAG*), der Terminalnummer (TID), der Stationsnummer (STAT_ID) und der Stations-Issuer-Nummer STAT_ISS gebildet wird.

[0068] Da beim 3DES-Verfahren mit Schlüssellängen von bis zu 112 Bit gearbeitet wird, ist die so ermittelte Ziffer zu lang, weshalb diese mittels MOD 0xF00000 und MOD 1000000 auf 6 Dezimalstellen trunkiert wird. Dieser 6-stellige Dezimalwert wird ferner in seinen letzten drei Stellen auf NULL mittels &0xFFF000 gesetzt. Zur Erzeugung der PIN_AT wird anstelle der letzten drei Ziffern die verschlüsselte Personalnummer PNR_RM* angehängt.

[0069] Der gesamte Vorgang der Erstellung der PIN_AT mit allen zugehörigen Parametern wird in der Zentrale 42 datenbanktechnisch archiviert. Im Betrugs- bzw. Manipulationsfall besteht jederzeit die Möglichkeit, die Kartenleserin-

betriebnahme lückenlos nachzuvollziehen. Die Daten werden in der Zentrale 42 mindestens 3 Jahre gespeichert. Hierbei können die Parameter Personal-Nr. des Technikers in der Zentrale PNR-RM, Personal-Nr. ServiceTechniker vor Ort PNR_ST, Terminal Id TID, Auftragsnummer AUFT_ID, Stationsnummer STAT_ID, Stationsissuer STAT_ISS, Zeitstempel DAT.

[0070] Die Zentrale 42 übermittelt (64) an den Servicetechniker 34 über das Kommunikationsnetz 38 die generierte Auftragsnummer AUFT_ID sowie die PIN_AT, die die verschlüsselte Personalnummer PNR_RM* enthält. Alternativ kann die Zentrale 42 diese Information auch unmittelbar an das PinPad 6 übertragen. Hierzu kann beispielsweise eine Mobilfunkverbindung zur Datenübertragung genutzt werden.

[0071] Der Servicetechniker 34 gibt in das PinPad 6 die soeben erhaltenen Daten ein (66). Der Servicetechniker 34 hat bereits seine Personalnummer PNR_ST dem PinPad 6 mitgeteilt (54). Im PinPad 6 kann mit den erhaltenen Informationen eine verschlüsselte Auftragsnummer AUFTRAG* mittels

$$AUFTRAG^{*} = (3DES_{e}\ K_{SB\_Key}(\ AUFT\_ID\ |\ PNR\_RM^{*}\ |\ S\&B\_ID\ |\ DAT)\ MOD\ 0xF00)$$

errechnet werden. Mit Hilfe der so ermittelten verschlüsselten Auftragsnummer AUFTRAG* kann eine PIN_AT im PinPad 6 mittels

$$PIN\_AT = (3DES_{e}\ K_{SB\_Key}(\ PNR\_ST\ |\ AUFTRAG^{*}\ |\ TID\ |\ STAT\_ID\ |\ STAT\_ISS)\ MOD\ 0xF00000)\ MOD\ 1000000)\ \&\ 0xFFF000)\ +\ PNR\_RM^{*})$$

errechnet werden.

[0072] Die in dem PinPad 6 errechnete PIN_AT wird mit der vom Servicetechniker 34 in das PinPad 6 eingegebenen PIN_AT verglichen (6). Bei einem positiven Vergleich wird dem Servicetechniker 34 die erfolgreiche Freigabe mitgeteilt (68) .

[0073] Darüber hinaus werden von dem PinPad 6 an den Kartenleser 10 über die Datenleitung 24 Schlüssel (Key) zur Entschlüsselung von PIN übertragen (70). Hierzu werden die Schlüssel (Key) aus dem Speicherbereich 14 über die Schnittstelle 20, die Datenleitung 24 und die Schnittstelle 22 an den Speicherbereich 18 übertragen. Bei dieser Übertragung der Schlüssel (Key) kann ebenfalls eine Verschlüsselung erfolgen. Die hierbei übertragenen sicherheitsrelevanten Daten, insbesondere die Schlüssel (Key) für die Offline-PIN-Überprüfung, unterscheiden sich regelmäßig von den Schlüsseln (K_{SB_Key}) für die Durchführung des oben geschilderten 4-Augen-Prinzips mittels 3DES.

[0074] Die 3DES-Verschlüsselung beruht darauf, dass die Schlüssel K_{SB_KEY} geheim sind. Sollten diese Schlüssel aus irgendwelchen Gründen nicht mehr geheim sein, so ist es möglich, mittels einer Fernübertragung neue Schlüssel K_{SB_KEY} in den Speicherbereich 14 des PinPads 6 zu laden, so dass nachfolgende Überprüfungen von PIN wieder sicher sind.

[0075] Das erfindungsgemäße Verfahren zeichnet sich insbesondere dadurch aus, dass die Kosten für einen zweiten Servicetechniker vor Ort eingespart werden können. Das erfindungsgemäße Verfahren zeichnet sich ferner dadurch aus, dass die Entitäten, die an der Freischaltung beteiligt sind, voneinander nichts wissen und somit sich einander nicht ausspähen können.

Patentansprüche

1. Verfahren zur Freigabe zumindest einer Einrichtung, bei dem die Freigabe zumindest teilweise durch mindestens einen ersten Code kontrolliert wird,
dadurch gekennzeichnet,
dass der erste Code mit Hilfe von Parametern von zumindest zwei Entitäten ermittelt wird.

2. Verfahren nach Anspruch 1,
dadurch gekennzeichnet,
dass zumindest zwei der Entitäten räumlich getrennt sind.

3. Verfahren nach einem der Ansprüche 1 bis 2,
dadurch gekennzeichnet,
dass mindestens eine Entität eine Person ist und dass die von dieser Entität ermittelten Parameter personenbezogene Parameter sind.

4. Verfahren nach einem der Ansprüche 1 bis 3,
dadurch gekennzeichnet,
dass mindestens eine Entität die freizugebende Einrichtung ist und dass die von dieser Entität ermittelten Parameter einrichtungsbezogene Parameter sind.

5. Verfahren nach einem der Ansprüche 1 bis 4,
dadurch gekennzeichnet,
dass die von einer Entität ermittelten Parameter zeitbezogene Parameter sind.

6. Verfahren nach einem der Ansprüche 1 bis 5,
dadurch gekennzeichnet,
dass die von einer Entität ermittelten Parameter auftragsbezogene Parameter sind.

7. Verfahren nach einem der Ansprüche 1 bis 6,
dadurch gekennzeichnet,
dass zumindest ein von einer einrichtungsseitigen Entität ermittelter Parameter an eine von der Einrichtung entfernte Zentrale übermittelt wird.

8. Verfahren nach einem der Ansprüche 1 bis 7,
dadurch gekennzeichnet,
dass für die Berechnung des ersten Codes mindestens ein von einer zentralseitigen Entität ermittelter Parameter und mindestens ein von der einrichtungsseitigen Entität ermittelter Parameter verwendet werden.

9. Verfahren nach Anspruch 8,
dadurch gekennzeichnet,
dass der mindestens eine von der zentralseitigen Entität ermittelte Parameter an die Einrichtung übermittelt wird.

10. Verfahren nach einem der Ansprüche 8 oder 9,
dadurch gekennzeichnet,
dass der mindestens eine von der zentralseitigen Entität ermittelte Parameter zumindest teilweise verschlüsselt wird.

11. Verfahren nach einem der Ansprüche 8 bis 10,
dadurch gekennzeichnet,
dass der zentralseitig berechnete erste Code an die Einrichtung übermittelt wird.

12. Verfahren nach einem der Ansprüche 8 bis 11,
dadurch gekennzeichnet,
dass der zentralseitig berechnete erste Code einrichtungsseitig zumindest mit Hilfe des mindestens einen von der Zentrale übermittelten zentralseitigen Parameters überprüft wird.

13. Verfahren nach einem der Ansprüche 8 bis 12,
dadurch gekennzeichnet,

dass der erste Code zentralseitig und einrichtungsseitig mit derselben Rechenvorschrift berechnet wird.

14. Verfahren nach einem der Ansprüche 1 bis 13,
dadurch gekennzeichnet,
dass zumindest der erste Code mit Hilfe eines symmetrischen Verschlüsselungsverfahrens berechnet wird.

15. Verfahren nach einem der Ansprüche 1 bis 14,
dadurch gekennzeichnet,
dass die Freigabe der Einrichtung zumindest durch den ersten Code und einen zweiten Code kontrolliert wird.

16. Verfahren nach Anspruch 15,
dadurch gekennzeichnet,
dass der zweite Code mit Hilfe von personenbezogenen Parametern ermittelt wird.

17. Verfahren nach einem der Ansprüche 15 oder 16,
dadurch gekennzeichnet,
dass der zweite Code zumindest mit Hilfe von mindestens einem personenbezogenen Parameter einrichtungsseitig überprüft wird.

18. Verfahren nach einem der Ansprüche 7 bis 17,
dadurch gekennzeichnet,
dass zumindest der erste Code über eine direkte elektronische Kommunikationsverbindung zwischen der Einrichtung und der Zentrale übermittelt wird.

19. Einrichtung umfassend

- Eingabemittel zur Eingabe von Parametern von zumindest zwei Entitäten und zur Eingabe mindestens eines ersten Codes, und
- Freigabemittel zur zumindest teilweisen Freigabe der Einrichtung bei positiver Überprüfung zumindest des ersten mit Hilfe von Parametern von zumindest zwei Entitäten ermittelten Codes.

20. Einrichtung nach Anspruch 19, **gekennzeichnet durch** Rechenmitteln zur Berechnung eines Vergleichscodes zumindest mit Hilfe der eingegebenen Parameter.

21. Einrichtung nach Anspruch 20, **gekennzeichnet durch** Vergleichsmittel zum Vergleichen des berechneten Vergleichscodes mit dem ersten Code.

22. Einrichtung nach Anspruch 21, **dadurch gekennzeichnet, dass** die Freigabemittel zur zumindest teilweisen Freigabe der Einrichtung bei Übereinstimmung zumindest des ersten Codes mit dem Vergleichscode eingerichtet sind.

23. Einrichtung nach einem der Ansprüche 20 bis 22,
dadurch gekennzeichnet,
dass die Rechenmittel zur Berechnung des Codes mittels einer symmetrischen Verschlüsselungsvorschrift eingerichtet sind.

24. System zur Berechung eines Freigabecodes,

- mit einer Einrichtung nach Anspruch 19 und
- einer Zentrale,

dadurch gekennzeichnet,

- **dass** die Zentrale zur Berechnung zumindest eines ersten Codes mit Hilfe von Parametern von zumindest zwei Entitäten eingerichtet ist.

25. Computerprogramm mit Instruktionen ausführbar auf einem Prozessor derart, dass zumindest eine Einrichtung freigegeben wird, wobei die Freigabe zumindest teilweise durch mindestens einen ersten Code kontrolliert wird und der erste Code mit Hilfe von Parametern von zumindest zwei Entitäten ermittelt wird.

26. Computerprogrammprodukt umfassend ein Computerprogramm mit Instruktionen ausführbar auf einem Prozessor derart, dass zumindest eine Einrichtung freigegeben wird, wobei die Freigabe zumindest teilweise durch mindestens einen ersten Code kontrolliert wird und der erste Code mit Hilfe von Parametern von zumindest zwei Entitäten ermittelt wird.

Geänderte Patentansprüche gemäss Regel 86(2) EPÜ.

1. Verfahren zur Freigabe zumindest einer Einrichtung, bei dem die Freigabe zumindest teilweise durch mindestens einen ersten Code kontrolliert wird,
dadurch gekennzeichnet,

- **dass** zumindest ein von einer einrichtungsseitigen Entität ermittelter Parameter an eine von der Einrichtung räumlich entfernte Zentrale übermittelt wird,
- **dass** der erste Code mit Hilfe mindestens eines von einer zentralseitigen Entität ermittelten Parameters und des mindestens einen von der einrichtungsseitigen Entität ermittelten Parameters berechnet wird,
- **dass** der mindestens eine von der zentralseitigen Entität ermittelte Parameter zusammen mit dem zentralseitig berechneten erste Code an die Einrichtung übermittelt wird, und
- **dass** der zentralseitig berechnete erste Code einrichtungsseitig zumindest mit Hilfe des mindestens einen von der Zentrale übermittelten zentralseitigen Parameters überprüft wird.

2. Verfahren nach Anspruch 1,
dadurch gekennzeichnet,
dass zumindest zwei der Entitäten räumlich getrennt sind.

3. Verfahren nach einem der Ansprüche 1 bis 2,
dadurch gekennzeichnet,
dass mindestens eine Entität eine Person ist und dass die von dieser Entität ermittelten Parameter personenbezogene Parameter sind.

4. Verfahren nach einem der Ansprüche 1 bis 3,
dadurch gekennzeichnet,
dass mindestens eine Entität die freizugebende Einrichtung ist und dass die von dieser Entität ermittelten Parameter einrichtungsbezogene Parameter sind.

5. Verfahren nach einem der Ansprüche 1 bis 4,
dadurch gekennzeichnet,
dass die von einer Entität ermittelten Parameter zeitbezogene Parameter sind.

6. Verfahren nach einem der Ansprüche 1 bis 5,
dadurch gekennzeichnet,
dass die von einer Entität ermittelten Parameter auftragsbezogene Parameter sind.

7. Verfahren nach einem der Ansprüche 1 bis 6,
dadurch gekennzeichnet,
dass der mindestens eine von der zentralseitigen Entität ermittelte Parameter zumindest teilweise verschlüsselt wird.

8. Verfahren nach einem der Ansprüche 1 bis 7,
dadurch gekennzeichnet,
dass der erste Code zentralseitig und einrichtungsseitig mit derselben Rechenvorschrift berechnet wird.

9. Verfahren nach einem der Ansprüche 1 bis 8,
dadurch gekennzeichnet,
dass zumindest der erste Code mit Hilfe eines symmetrischen Verschlüsselungsverfahrens berechnet wird.

10. Verfahren nach einem der Ansprüche 1 bis 9,
dadurch gekennzeichnet,
dass die Freigabe der Einrichtung zumindest durch den ersten Code und einen zweiten Code kontrolliert wird.

11. Verfahren nach Anspruch 10,
dadurch gekennzeichnet,
dass der zweite Code mit Hilfe von personenbezogenen Parametern ermittelt wird.

12. Verfahren nach einem der Ansprüche 10 oder 11,
dadurch gekennzeichnet,
dass der zweite Code zumindest mit Hilfe von mindestens einem personenbezogenen Parameter einrichtungsseitig überprüft wird.

13. Verfahren nach einem der Ansprüche 1 bis 12,
dadurch gekennzeichnet,
dass zumindest der erste Code über eine direkte elektronische Kommunikationsverbindung zwischen der Einrichtung und der Zentrale übermittelt wird.

14. System zur Berechung eines Freigabecodes,

- mit einer Einrichtung umfassend
- Mittel zur Ausgabe eines einrichtungsseitigen Parameters,
- Eingabemittel zur Eingabe mindestens eines von einer zentralseitigen Entität ermittelten Parameters und des mindestens einen von der einrichtungsseitigen Entität ermittelten Parameters berechneten Codes, und
- Freigabemittel zur zumindest teilweisen Freigabe der Einrichtung bei positiver Überprüfung des Codes mit mindestens dem einen von der Zentrale übermittelten zentralseitigen Parameters und
- einer räumlich von der Einrichtung getrennten Zentrale,

dadurch gekennzeichnet,

- **dass** die Zentrale zur Berechnung des ersten Codes mit Hilfe mindestens eines von der Zentrale ermittelten Parameters und mindestens eines von der Einrichtung ermittelten Parameters, und zur gemeinsamen Übermittlung des mindestens einen von der Zentrale ermittelten Parameters und des zentralseitig berechneten ersten Codes an die Einrichtung eingerichtet ist.

15. System nach Anspruch 14, **gekennzeichnet durch** einrichtungsseitige Rechenmittel zur Berechnung eines Vergleichscodes zumindest mit Hilfe der eingegebenen Parameter.

16. System nach Anspruch 14, **gekennzeichnet durch** einrichtungsseitige Vergleichsmittel zum Vergleichen des berechneten Vergleichscodes mit dem ersten Code.

17. System nach Anspruch 14, **dadurch gekennzeichnet, dass** die Freigabemittel zur zumindest teilweisen Freigabe der Einrichtung bei Übereinstimmung zumindest des ersten Codes mit dem Vergleichscode eingerichtet sind.

18. System nach einem der Ansprüche 15 bis 17,
dadurch gekennzeichnet,
dass die Rechenmittel zur Berechnung des Codes mittels einer symmetrischen Verschlüsselungsvorschrift eingerichtet sind.

19. Computerprogramm mit Instruktionen ausführbar auf einem Prozessor derart, dass zumindest eine Einrichtung eines Systems nach Anspruch 14 mittels eines Verfahrens nach Anspruch 1 freigegeben wird.

20. Computerprogrammprodukt umfassend ein Computerprogramm mit Instruktionen ausführbar auf einem Prozessor derart, dass zumindest eine Einrichtung eines Systems nach Anspruch 14 mittels eines Verfahrens nach Anspruch 1 freigegeben wird.

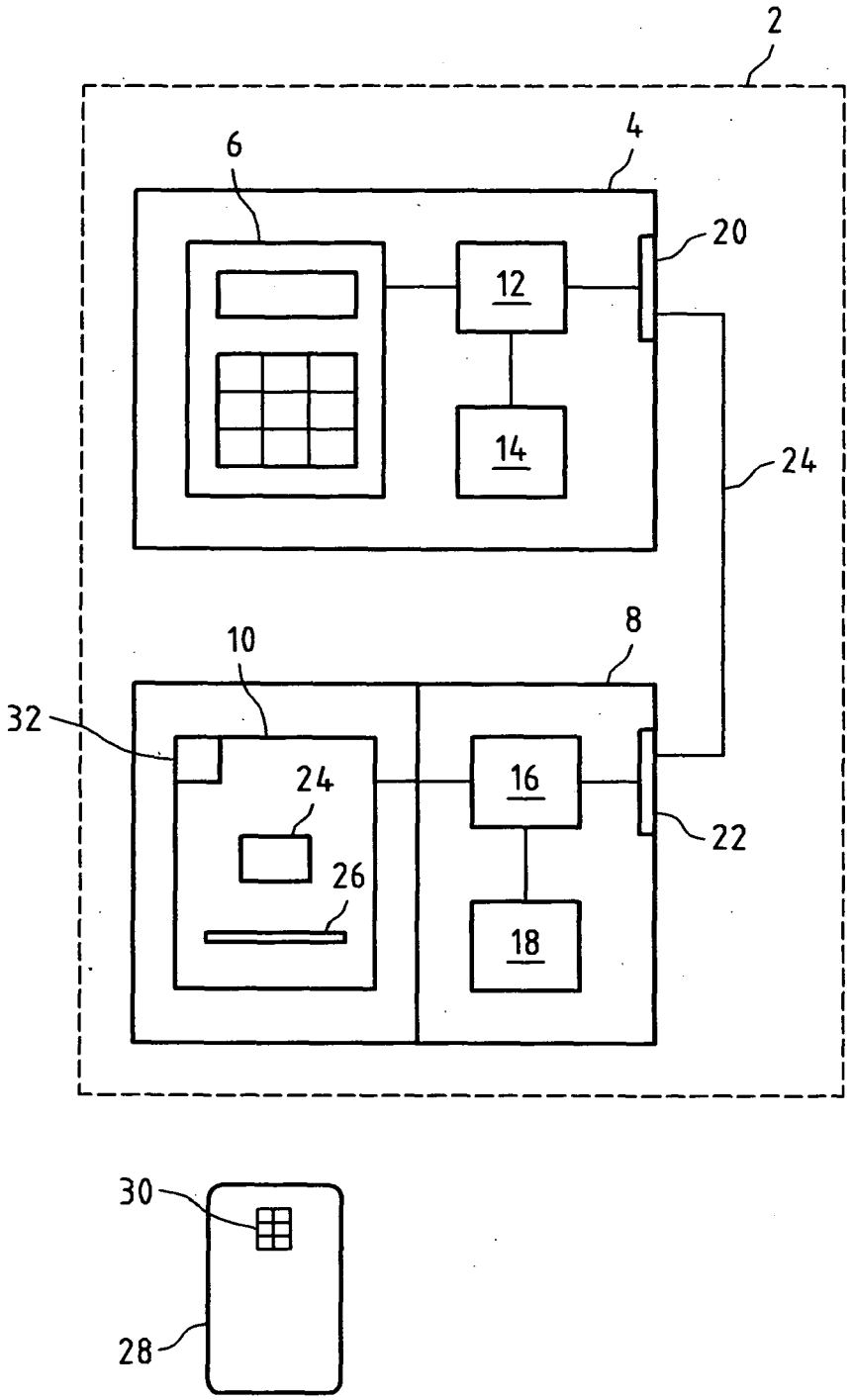

Fig.1

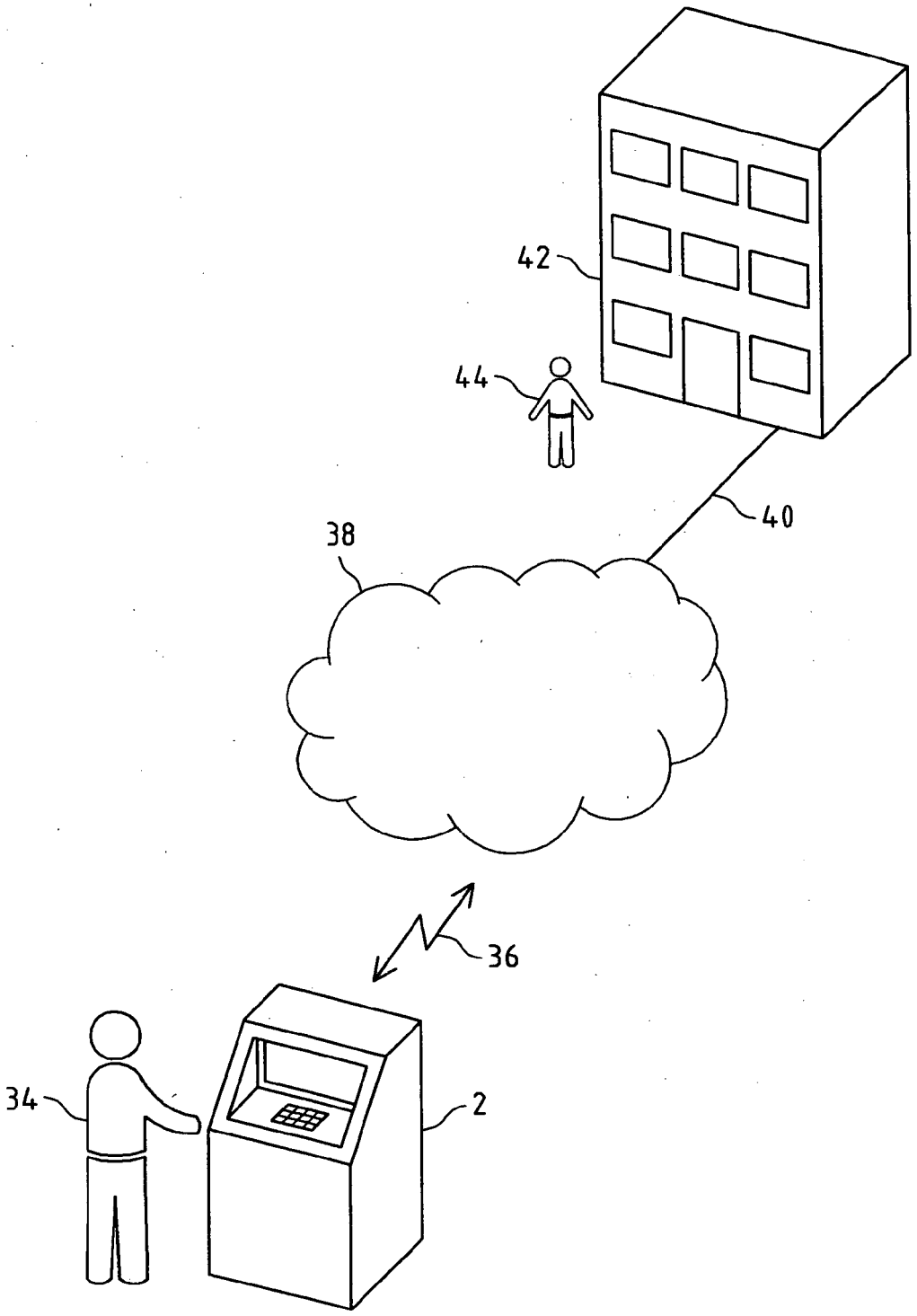

Fig.2

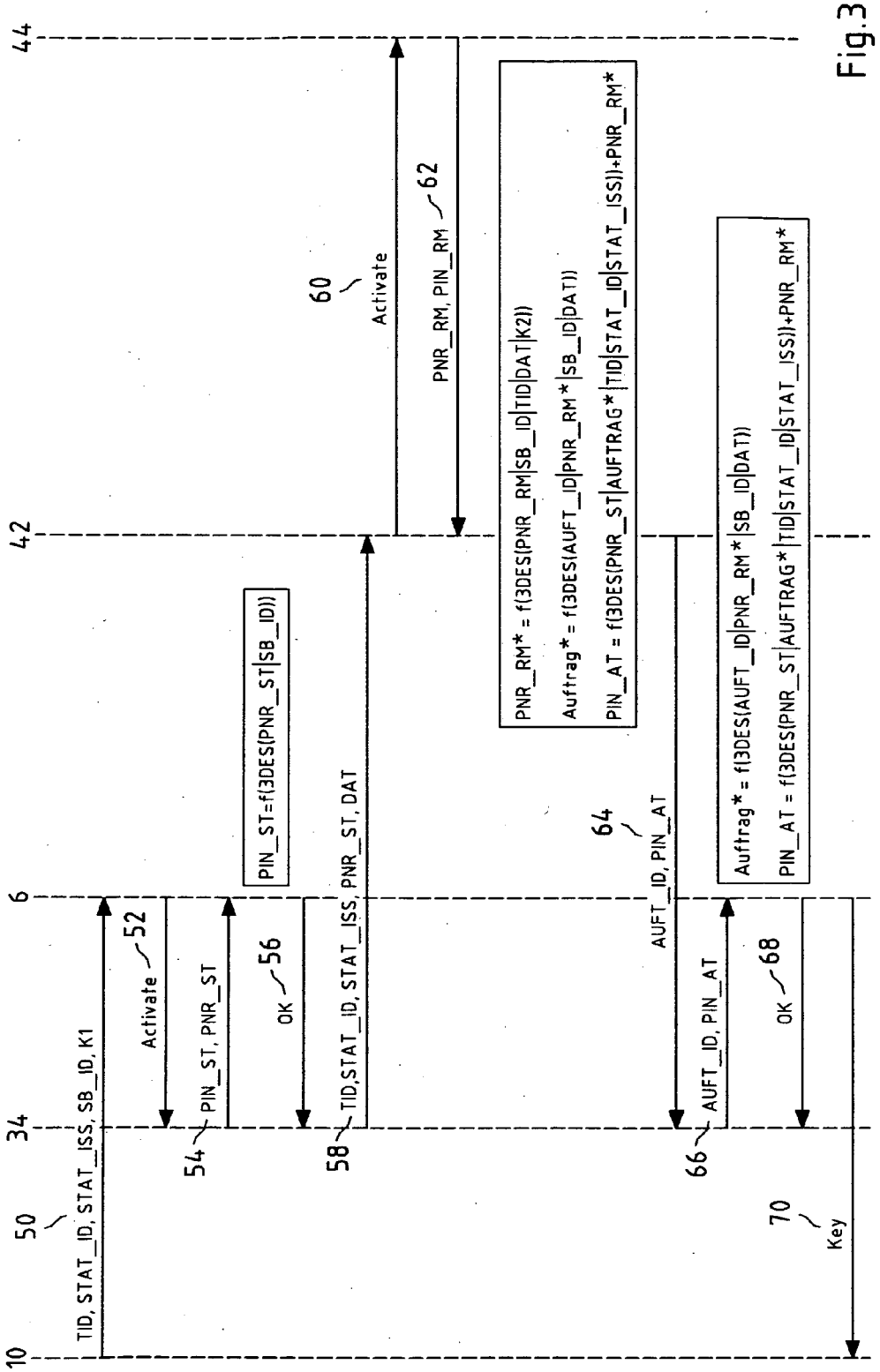
44
42
6
34
10
50
60
Activate
PNR_RM, PIN_RM
62
PIN_ST=f(3DES(PNR_ST|SB_ID))
PNR_RM* = f(3DES(PNR_RM|SB_ID|TID|DAT|K2))
Auftrag* = f(3DES(AUFT_ID|PNR_RM*|SB_ID|DAT))
PIN_AT = f(3DES(PNR_ST|AUFTRAG*|TID|STAT_ID|STAT_ISS))+PNR_RM*
64
AUFT_ID, PIN_AT
Auftrag* = f(3DES(AUFT_ID|PNR_RM*|SB_ID|DAT))
PIN_AT = f(3DES(PNR_ST|AUFTRAG*|TID|STAT_ID|STAT_ISS))+PNR_RM*
TID, STAT_ID, STAT_ISS, SB_ID, K1
Activate
52
PIN_ST, PNR_ST
54
OK
56
TID,STAT_ID, STAT_ISS, PNR_ST, DAT
58
AUFT_ID, PIN_AT
66
OK
68
70
Key

Fig.3

Europäisches Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 05 00 7519

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int.Cl.7)
X	US 5 668 876 A (FALK ET AL) 16. September 1997 (1997-09-16) * Zusammenfassung * * Spalte 2, Zeilen 6-13 * * Spalte 2, Zeile 65 - Spalte 3, Zeile 20 * * Spalte 4, Zeile 1 - Spalte 5, Zeile 7 * * Spalte 5, Zeile 29 - Spalte 6, Zeile 2 * * Abbildungen *	1-26	G07F19/00
X	BE 1 006 817 A6 (LAUREYSSENS DIRK; DE BECKER HARRY; DIRIX WERNER) 13. Dezember 1994 (1994-12-13) * Zusammenfassung * * Seite 2, Zeile 2 - Seite 3, Zeile 25 * * Anspruch 1 *	1-26	
X	EP 1 260 659 A (BURG-WAECHTER KG) 27. November 2002 (2002-11-27) * Zusammenfassung * * Absätze [0034] - [0037] * * Anspruch 1 *	1-26	RECHERCHIERTE SACHGEBIETE (Int.Cl.7) G07F G07C
X	RANKL W ET AL: "Handbuch der Chipkarten, PASSAGE" HANDBUCH DER CHIPKARTEN. AUFBAU - FUNKTIONSWEISE - EINSATZ VON SMART CARDS, MUENCHEN : CARL HANSER VERLAG, DE, 1999, Seiten 450-459, XP002268702 ISBN: 3-446-21115-2 * Zusammenfassung * * Seiten 455-458 *	1-26	
A	WO 2004/056030 A (WINCOR NIXDORF INTERNATIONAL GMBH; NOLTE, MICHAEL) 1. Juli 2004 (2004-07-01) * Zusammenfassung *	1-26	

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
Den Haag	21. Juli 2005	Breugelmans, J

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus anderen Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

3

EPO FORM 1503 03.82 (P04C03)

ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR. EP 05 00 7519

In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten europäischen Recherchenbericht angeführten Patentdokumente angegeben.
Die Angaben über die Familienmitglieder entsprechen dem Stand der Datei des Europäischen Patentamts am
Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

21-07-2005

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 5668876 A	16-09-1997	AU 692881 B2	18-06-1998
		AU 2688795 A	19-01-1996
		CA 2193819 A1	04-01-1996
		CN 1156531 A ,C	06-08-1997
		EP 0766902 A2	09-04-1997
		FI 965161 A	13-02-1997
		JP 10502195 T	24-02-1998
		WO 9600485 A2	04-01-1996
BE 1006817 A6	13-12-1994	KEINE	
EP 1260659 A	27-11-2002	DE 10128146 A1	12-12-2002
		EP 1260659 A2	27-11-2002
WO 2004056030 A	01-07-2004	DE 10259270 A1	15-07-2004
		WO 2004056030 A2	01-07-2004

EPO FORM P0461

Für nähere Einzelheiten zu diesem Anhang : siehe Amtsblatt des Europäischen Patentamts, Nr.12/82