(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 10 2006 057 093 B4** 2008.10.02

(12) # Patentschrift

(21) Aktenzeichen: **10 2006 057 093.6**
(22) Anmeldetag: **04.12.2006**
(43) Offenlegungstag: **05.06.2008**
(45) Veröffentlichungstag der Patenterteilung: **02.10.2008**

(51) Int Cl.[8]: ***H04L 9/32*** (2006.01)

(73) Patentinhaber:
Infineon Technologies AG, 81669 München, DE

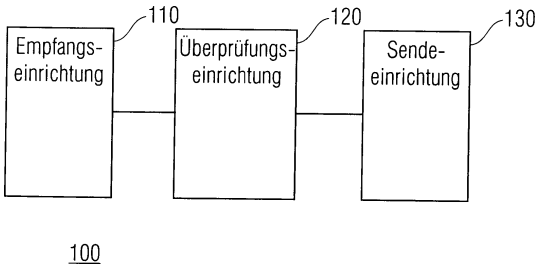
(74) Vertreter:
Schoppe, Zimmermann, Stöckeler & Zinkler, 82049 Pullach

(72) Erfinder:
Riegebauer, Josef, Ilz, AT

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:
US2006/02 08 066 A1
US2005/00 86 497 A1
Mifare(R) Standard Card IC MF1 IC S50. Functional Specification, Produkt Specification Rev. 5.0, Philips Semiconductors, November 1999, S. 1-19;
Security & Chip Card ICs SLE 55R16, Intelligent 2560-Byte EEPROM with Contactiess Interface com-
plying to ISO/IEC 14443 Type A and Security Logic.
Short Product Information, Infineon Technologies, Januar 2001, S. 1-8;

(54) Bezeichnung: **Vorrichtung zur Auswahl einer virtuellen Kartenanwendung**

(57) Hauptanspruch: Vorrichtung (100) zur Auswahl einer Anwendung eines Geräts, mit folgenden Merkmalen:
einer Empfangseinrichtung (110) zum Empfangen eines Authentisierungskommandos, aus dem Informationen über einen Schlüssel eines Lesegeräts, das mit dem Gerät kommuniziert, ableitbar sind;
einer Überprüfungseinrichtung (120), um anhand der Informationen aus dem Authentisierungskommando solange zu überprüfen, ob eine der Anwendungen und das Lesegerät einen gemeinsamen Schlüssel verwenden, bis eine Schlüsselübereinstimmung gefunden ist oder alle Anwendungen überprüft sind und zur Selektion einer Anwendung für eine Kommunikation mit dem Lesegerät anhand der Schlüsselübereinstimmung, wobei die Überprüfungseinrichtung (120) ausgebildet ist, um zur Selektion der Anwendung die Anwendungen sequentiell zu überprüfen und Anwendungen mit einer erfolglosen Überprüfung temporär von der Überprüfung auszuschließen; und
einer Sendeeinrichtung (130) zum Senden einer Antwort der selektierten Anwendung an das Lesegerät.



Beschreibung

Hintergrund

[0001] Die vorliegende Erfindung bezieht sich auf eine Vorrichtung zur Auswahl einer virtuellen Kartenanwendung, wie sie beispielsweise in Mobilfunktelefonen oder portablen Computern, die Kartenemulation unterstützen, zum Einsatz kommen.

[0002] Moderne Kontaktloskarten, sog. Smartcards, oder auch NFC-taugliche (NFC = Near Field Communication) mobile Geräte, wie beispielsweise Mobilfunktelefone, PDAs (PDA = Personal Digital Assistant) mit einem Kontaktlos-Subsystem, welches Kartenemulation unterstützt, können mehrere Kontaktlos-Applikationen emulieren. Eine solche Kontaktlos-Applikation stellt für sich eine „virtuelle" Kontaktloskarte dar, wobei diese aber nach außen hin nur für die Dauer einer Kontaktlos-Transaktion als „physikalische Karte" sichtbar ist, um zu bestehenden Kontaktlos-Leser-Infrastrukturen (Legacy Systeme) kompatibel zu sein.

[0003] Die in der konventionellen Technik weltweit installierten „Legacy Systeme" unterstützen das Konzept „virtueller Karten" nicht. Aus der konventionellen Technik ist der Begriff „Anticollision" bekannt und bezieht sich auf die Selektion einer physikalischen Karte aus einer Mehrzahl von physikalischen Karten, die gleichzeitig einem Kontaktlos-Leser präsentiert werden. Eine eindeutige Selektion und Aktivierung einer entsprechenden virtuellen Karte ohne Eingriff in bestehende Infrastrukturen und unter Wahrung der Konformität zu existierenden Standards, also auf sämtlichen physikalischen und logischen Schichten der Kontaktlos-Protokolle, ist im Rahmen der konventionellen Technik innerhalb eines Protokolls nicht vorgesehen. Eine Auswahl solcher Applikationen kann über unterschiedliche RF-Kommunikationstechnologien geschehen (RF = Radio Frequency), wie beispielsweise durch ISO 14443 Typ A, Typ B, ISO 18092 oder ISO 15693, usw.

[0004] Die konventionelle Technologie kennt ferner ein Auswahlverfahren einer Applikation innerhalb der gleichen Kommunikationstechnologie, oder des gleichen Protokolls, durch Unterscheidung in einem globalen Applikationsidentifikator (AID = Applikationsidentifikator), wie es im ISO 7816-5 beschrieben ist.

[0005] Ferner ist es möglich, aus Applikationen in der gleichen RF-Kommunikationstechnologie durch unterschiedliche Protokolle zur Bedienung der Karte auszuwählen, wie beispielsweise eine ISO 14443-4 Applikation gegenüber proprietären Schemen wie beispielsweise Mifare oder My-D, wobei alle die RF-Kommunikationstechnologie ISO 14443-3 Typ A verwenden, sich aber in der Kodierung der Kommandos unterscheiden.

[0006] Ein Auswahlverfahren durch Informationen von externen Geräten, wie beispielsweise eine Identifikation der Zielapplikation aus einer Kontextinformation heraus, die beispielsweise von einem Mobilfunktelefon via RFID (RFID = Radio Frequency Identifikation, Bluetooth, usw. mitgeteilt wurde, ist prinzipiell denkbar, insofern, dass die Mittel zum Empfangen zur Verarbeitung der Kontextinformation vorhanden sind. Die konventionelle Technik bietet jedoch kein Verfahren, welches in der Lage wäre, basierend auf den gleichen Protokollen und ohne Modifikation der gleichen eine Applikation in der gleichen Kommunikationstechnologie, wie beispielsweise ISO 14443 Typ A, zu unterscheiden. Eine Verwaltung mehrerer virtueller Karten ist somit nicht möglich, bzw. nur mit einer deutlich höheren Komplexität auf Infrastrukturebene, um die konventionellen Verfahren zu ermöglichen.

[0007] Die US 2005/0086497 A1 offenbart ein Konzept zur Absicherung von Daten, mit Hilfe einer IC-Karte. Das Konzept sieht vor, Nutzdaten zu verschlüsseln und an einem bestimmten Ort, beispielsweise im Internet, zu speichern. Zugangsdaten, d. h. die zur Entschlüsselung notwendigen Schlüssel sowie Informationen über den Ort, an dem die Daten gespeichert sind, werden dann auf der IC-Karte gespeichert. Damit sind alle sicherheitsrelevanten Daten auf der IC-Karte gespeichert. Ein Zugriff auf diese Daten ohne die IC-Karte ist nicht möglich. Da nur Zugangsdaten in Form von Schlüsseln usw. auf der Karte gespeichert werden, wird somit Speicherplatz eingespart, da die eigentlichen Nutzdaten ausgelagert werden.

[0008] Philips bietet mit dem MF1 IC S50 einen Mifare-Chip dem Markt an, der zur kontaktlosen Übertragung von Daten und Energie in der Lage ist. Der Chip kann mit Energie aus einem elektromagnetischen Feld betrieben werden.

[0009] Auch Infineon bietet ICs, wie beispielsweise den SLE 55R16, der ein intelligentes EEPROM mit einer Schnurlosschnittstelle kompatibel zum ISO/IEC 14443 Typ A Standard bereitstellt.

[0010] Die US 2006/0208066 A1 offenbart ein RFID-Modul, das ferner Schnittstellen zur Kommunikation mit Servern und Netzwerken, beispielsweise über USB-Schnittstellen, aufweist. Das Modul kann dabei sowohl Schnittstellen zur schnurlosen Kommunikation als auch kontaktgebundene Schnittstellen aufweisen.

Zusammenfassung

[0011] Ausführungsbeispiele der Erfindung umfassen eine Vorrichtung zur Auswahl einer virtuellen Anwendung eines multiapplikationstauglichen Geräts, mit einer Empfangseinrichtung zum Empfangen ei-

nes Authentisierungskommandos, aus dem Informationen über einen Schlüssel eines Lesegeräts ableitbar sind, einer Überprüfungseinrichtung, um anhand der Informationen aus dem Authentisierungskommando zu überprüfen, ob eine der virtuellen Anwendungen und das Lesegerät einen gemeinsamen Schlüssel verwenden, und zur Selektion einer Anwendung für eine Kommunikation mit dem Lesegerät anhand einer Schlüsselübereinstimmung, und einer Sendeeinrichtung (**130**) zum Senden einer Antwort der selektierten Anwendung an das Lesegerät.

Kurzbeschreibung der Figuren

[0012] Bevorzugte Ausführungsbeispiele der vorliegenden Erfindung werden nachfolgend bezugnehmend auf die beiliegenden Zeichnungen näher erläutert. Es zeigen:

[0013] Fig. 1 ein Ausführungsbeispiel einer Vorrichtung zur Auswahl einer virtuellen Kartenanwendung;

[0014] Fig. 2a ein Ausführungsbeispiel einer Selektionsschaltung;

[0015] Fig. 2b ein weiteres Ausführungsbeispiel einer Selektionsschaltung; und

[0016] Fig. 3 ein Ausführungsbeispiel eines Verfahrens zur Auswahl einer virtuellen Kartenapplikation.

Detaillierte Beschreibung

[0017] Bevor im folgenden Ausführungsbeispiele der vorliegenden Erfindung anhand der Zeichnungen näher erläutert werden, wird darauf hingewiesen, dass gleiche Elemente in den Figuren mit den gleichen oder ähnlichen Bezugszeichen versehen sind und dass eine wiederholte Beschreibung dieser Elemente weggelassen wird.

[0018] Ausführungsbeispiele machen sich einen gegenseitigen Authentisierungsmechanismus, der beispielsweise von Applikationen verwendet werden kann, die einen kryptographischen Algorithmus verwenden, wie beispielsweise My-D, Mifare Classic, bevor eine Kommunikation mit einem Kontaktlosleser aufgenommen wird, zu Nutze. Ausführungsbeispiele eignen sich deswegen auch für NFC-Geräte im energetischen Betriebszustand „Emergency Mode", in diesem Fall wird die Energie für das Kontaktlossubsystem ausschließlich aus dem RF-Feld bezogen, eine Benutzerschnittstelle, wie beispielsweise eine Tastatur oder ein Bildschirm, stehen für die Applikationsauswahl dann nicht zur Verfügung. Ausführungsbeispiele limitieren die Anzahl der virtuellen Karten aus denen ausgewählt werden nicht wesentlich. Nach Empfang des Authentisierungskommandos durchsuchen Ausführungsbeispiele vorhandene virtuelle Karten auf Schlüsselübereinstimmungen. Dies kann beispielsweise durch einen Assoziationsalgorithmus, der sowohl in Hardware als auch in Software implementiert sein kann, realisiert werden. Bei Übereinstimmung wird die entsprechende virtuelle Karte selektiert und eine Antwort an den Kartenleser zurückgesendet. In praktischen Anwendungsfällen sind aufgrund der üblichen Schlüsselraumdimensionen mehrfache Übereinstimmungen weitgehend auszuschließen.

[0019] Andere Ausführungsbeispiele durchsuchen die virtuellen Karten in Einzeltransaktionen, das heißt, sie überprüfen nach dem Empfang eines Authentisierungskommandos nur eine virtuelle Karte auf Schlüsselübereinstimmung und senden bei Nichtübereinstimmung keine Antwort an den Kartenleser. Ferner kann für die ausgeschlossene Karte ein Indikator in einem nichtflüchtigen Speicher abgelegt werden, so dass Ausführungsbeispiele im Folgenden diese Karte temporär nicht mehr überprüfen. Es kann davon ausgegangen werden, dass ein Kontaktlosleser nach einem Time-out, oder ggf. auch nach einem RF-Feldreset, eine neue Anti-Kollision durchführt, das heißt, ein entsprechendes Authentisierungskommando wiederholt. Das wiederholte Authentisierungskommando beinhaltet dann in einer üblichen Implementierung die gleiche Schlüsselinformation.

[0020] Seitens des Ausführungsbeispiels kann nun im Rahmen der Multiapplikationskarte eine frei wählbare Strategie implementiert werden, nach der eine andere als die zuletzt erfolglos überprüfte virtuelle Karte zur Authentisierung ausgewählt wird. Ausführungsbeispiele, die beispielsweise den beschriebenen Authentisierungsmechanismus umfassen, können somit eine signifikante Anzahl von bestehenden Systemen im Markt bedienen. Ferner kann davon ausgegangen werden, dass eine eventuelle Verzögerung, die durch die Individualüberprüfungen der einzelnen virtuellen Karten hervorgerufen wird, im Bereich weniger Millisekunden liegt und somit als unrelevant erachtet werden kann. In anderen Ausführungsbeispielen können auch parallele Überprüfungsroutinen realisiert werden.

[0021] Ausführungsbeispiele realisieren somit ein Verfahren für die Selektion einer Emulation einer bestimmten virtuellen Kartenapplikation aus einer Mehrzahl von kontaktlosen virtuellen Kartenanwendungen einer Multiapplikation-Kontaktloskarte oder eines Kontaktlos-Subsystems eines NFC-Gerätes ohne Benutzerinterface. Ausführungsbeispiele können angepasst sein auf Applikationen ohne Unterscheidungsmerkmale in ihrer Kontaktlos-Technologie oder ihrem Protokoll, speziell auch auf Applikationstypen, die Authentisierungsmechanismen verwenden.

[0022] Fig. 1 zeigt ein Ausführungsbeispiel einer Vorrichtung **100** zur Auswahl einer virtuellen Karten-

anwendung aus einer Multiapplikations-Kontaktloskarte. Die Vorrichtung **100** umfasst eine Empfangseinrichtung **110** zum Empfangen eines Authentisierungskommandos, aus dem Informationen über einen Schlüssel eines Kartenlesers ableitbar sind. Ferner weist die Vorrichtung **100** eine Überprüfungseinrichtung **120**), um anhand der Informationen aus dem Authentisierungskommando zu überprüfen, ob eine der virtuellen Kartenanwendungen und der Kartenleser einen gemeinsamen Schlüssel verwenden und zur Selektion einer Kartenanwendung für eine Kommunikation mit dem Kartenleser anhand einer Schlüsselübereinstimmung. Die Vorrichtung **100** umfasst ferner eine Sendeeinrichtung **130** zum Senden einer Antwort der selektierten Kartenanwendungen an den Kartenleser. Gemäß Ausführungsbeispielen enthält das Authentisierungskommando eine Nachricht, die mit dem gemeinsamen Schlüssel des Kartenlesers und der Karte bzw. einer der Anwendungen auf der Karte verschlüsselt ist, so dass die Karte z. B. entsprechend dem ISO 9798-2 feststellen kann, ob die Nachricht mit einem gemeinsamen Schlüssel verschlüsselt wurde.

[0023] In einem weiteren Ausführungsbeispiel kann die Überprüfungseinrichtung **120** ferner eine Emulationseinrichtung zur Emulation der selektierten Kartenanwendung und zum Generieren einer Antwort der selektierten Kartenanwendung aufweisen. Ferner kann eine Einrichtung zum Speichern der virtuellen Kartenanwendungen vorhanden sein. Ausführungsbeispiele können beispielsweise in portablen Geräten, wie Mobilfunktelefonen, PDAs oder portablen Computern implementiert sein. In einem Ausführungsbeispiel kann die Überprüfungseinrichtung **120** ausgebildet sein, um zur Selektion der Kartenanwendung die virtuellen Kartenanwendungen simultan zu überprüfen und diejenige Kartenanwendung zu selektieren, die eine Schlüsselübereinstimmung liefert. Ferner kann die Überprüfungseinrichtung **120** zur Selektion der Kartenanwendung die virtuellen Kartenanwendungen sequentiell überprüfen und Kartenanwendungen mit einer erfolglosen Überprüfung temporär von der Überprüfung ausschließen, um so in mehreren Überprüfungsintervallen zum Ziel zu gelangen.

[0024] Die Vorrichtung **100** und insbesondere die Einrichtung zum Empfangen **110** können in Ausführungsbeispielen ausgelegt sein, um Signale gemäß zumindest einem der ISO 14443 Typ A, ISO 14443 Typ B, ISO 18092 oder ISO 15693 zu empfangen und die Sendeeinrichtung **130** kann ebenfalls ausgebildet sein, um Signale gemäß zumindest einem dieser Standards zu senden. Ferner kann die Überprüfungseinrichtung **120** ausgebildet sein, um die Kartenanwendungen gemäß einem Authentisierungsmechanismus gemäß ISO 9798-2 zu überprüfen.

[0025] Fig. 2a zeigt ein Ausführungsbeispiel einer Selektionsschaltung **200**. Die Selektionsschaltung **200** umfasst einen Empfänger **210**, der mit einer Empfangsantenne **215** gekoppelt ist und einen Ausgang **218** für ein Empfangssignal aufweist. Der Überprüfer **220** umfasst einen Eingang **225**, der mit dem Ausgang **218** für das Empfangssignal gekoppelt ist und mit einem Ausgang **228** für ein Antwortsignal. Der Sender **220** umfasst einen Eingang **238**, der mit dem Ausgang **228** für das Antwortsignal gekoppelt ist.

[0026] In einem anderen Ausführungsbeispiel kann der Überprüfer **220** ferner eine Schnittstelle für eine Mehrzahl von virtuellen Kartenanwendungen aufweisen, die mit einer Multiapplikationscontrollerkarte koppelbar ist, so dass in einem anderen Ausführungsbeispiel der Überprüfer **220** mit einer Multiapplikationscontrollerkarte gekoppelt ist.

[0027] Ferner kann ein Ausführungsbeispiel eine Multiapplikationscontrollerkarte mit einem Speicher aufweisen, indem wenigstens eine virtuelle Kartenanwendung speicherbar ist. Die Selektionsschaltung **200** kann beispielsweise in ein portables Gerät integriert sein, wobei Mobilfunktelefone, PDAs, portable Computer usw. denkbar sind.

[0028] In einem weiteren Ausführungsbeispiel kann der Überprüfer **220** ferner einen Emulator aufweisen, mit einem Eingang für das Empfangssignal, einem Selektionseingang und einem Ausgang für das Antwortsignal. Der Emulator kann dann die selektierte Kartenanwendung emulieren und somit das Antwortsignal generieren. Der Empfänger **210** kann in Ausführungsbeispielen derart ausgelegt sein, dass an seinem Ausgang **218** für das Empfangssignal ein Empfangssignal gemäß zumindest einem der ISO 14443 Typ A, ISO 14443 Typ B, ISO 18092 oder ISO 15693 empfangen werden kann, und der Sender wiederum ausgebildet sein kann, um entsprechende Signale dieser Standards zu senden. Entsprechend ist in solchen Ausführungsbeispielen auch das Antwortsignal an die Spezifikationen dieser Standards angepasst.

[0029] Die Fig. 2b zeigt ein weiteres Ausführungsbeispiel einer Selektionsschaltung **300** mit einem Empfänger **210** mit einem Ausgang **218** an dem ein Empfangssignal ist, aus dem Informationen über einen Authentisierungsschlüssel ableitbar sind. Die Selektionsschaltung **200** weist ferner einen Überprüfer **220** auf, mit einem Eingang **225**, der mit dem Ausgang **218** des Empfängers **210** gekoppelt ist, einer Schnittstelle **229** für mehrere virtuelle Kartenanwendungen über die der Authentisierungsschlüssel verifizierbar ist, und mit einem Ausgang **228** für ein Antwortsignal einer virtuellen Kartenanwendung, für die der Authentisierungsschlüssel verifizierbar ist. Die Selektionsschaltung **300** weist ferner eine Multiapplikationscontrollerkarte **240** auf, die mit der Schnittstel-

le **229** für mehrere virtuelle Kartenanwendungen gekoppelt ist und einen Speicher umfasst, der wenigstens zwei virtuelle Kartenanwendungen speichert. Die Selektionsschaltung **300** umfasst ferner einen Sender **230**, mit einem Eingang **238**, der mit dem Ausgang **228** für das Antwortsignal gekoppelt ist. Optional können der Empfänger **210** an eine Empfangsantenne **215** und der Sender **230** an eine Senderantenne **235** gekoppelt sein.

[0030] In einem anderen Ausführungsbeispiel kann der Überprüfer **220** einen Emulator umfassen, der das Antwortsignal durch Emulation der virtuellen Kartenanwendung für die der Authentisierungsschlüssel verifizierbar ist, bereitstellt. Ferner kann die Multiapplikationscontrollerkarte **240** virtuelle Kartenanwendungen oder Kartenapplikationen der gleichen Art oder in der gleichen Kommunikationstechnologie speichern.

[0031] In einem weiteren Ausführungsbeispiel kann der Überprüfer **220** ausgebildet sein, um den Authentisierungsschlüssel unter Verwendung eines Protokolls zu verifizieren, wobei das Protokoll beispielsweise einem der Mifare Classic, oder My-D Standards entspricht (Mifare Classic ist eine Marke von Philips/NXP, My-D ist eine Trademark von Infineon Technologies). In anderen Ausführungsbeispielen kann der Überprüfer ferner zur Verifikation des Authentisierungsschlüssels Indikatoren für Kartenanwendungen mit fehlgeschlagenen Verifikationen temporär speichern, so dass diese Kartenanwendungen für einen gewissen Zeitraum von Überprüfungen ausgeschlossen sind.

[0032] Gemäß obigen Ausführungen kann die Selektionsschaltung, insbesondere der Empfänger **210** und der Sender **230** ausgelegt sein, um gemäß einem der ISO 14443 Typ A, ISO 14443 Typ B, ISO 18092 oder ISO 15693 zu kommunizieren. Ferner kann der Überprüfer **220** ausgelegt sein, um den Authentisierungsschlüssel gemäß ISO 9798-2 zu verifizieren.

[0033] Die Fig. 3 zeigt ein Flussdiagramm **400**, das ein Ausführungsbeispiel eines Verfahrens verdeutlicht. Das Verfahren beginnt in einem Schritt **400**, indem ein betreffendes Protokoll, wie beispielsweise ISO 14443 Typ A ausgewählt wird. Über die Antikollisionsprozedur und Selektion, die in einem Schritt **420** durchgeführt werden, wird die entsprechende Kommunikation mit einer virtuellen Kartenanwendung vorbereitet. In einem Schritt **430** werden nun die entsprechenden Layer 4 Protokolle ausgesucht, wobei die Fig. 3 auf der linken Seite **440** ein konventionelles Verfahren zeigt, das aus mehreren Applikationen mittels einer Applikationsidentifikation (AID) eine Applikation aussucht. Ein Ausführungsbeispiel ist unter **450** dargestellt, wo verschiedene Mifare Classic Applikationen dargestellt sind, die jeweils über andere Schlüssel verfügen. Durch Ausprobieren des für die Übertragung verwendeten Authentisierungsschlüssels an den verschiedenen Mifare Classic Applikationen wird die gesuchte Applikation identifiziert.

[0034] Ein Ausführungsbeispiel kann in einem NFC-Gerät realisiert sein, das ein Kontaktlos-Subsystem mit einem NFC-Modem zur Abwicklung einer Kontaktlos-Kommunikation aufweist. Ferner kann das NFC-Gerät ein Secure-Element, beispielsweise eine SIM-Karte mit einem geeigneten Betriebssystem, aufweisen. Eine Mehrzahl von kontaktlosen virtuellen Kartenapplikationen, z. B. fünf „Mifare Classic"-Applikationen, die beispielsweise die 3-Pass-Authentication nach ISO 9798-2 verwenden, können als „virtuelle Karten" in einem NVM (NVM = Non Volatile Memory) Speicher abgebildet sein. Nach Antikollision, vergl. Schritt **420** in der Fig. 3, wird das Authentisierungskommando für „Mifare Classic" empfangen und ein Authentisierungsmechanismus, eine sog. „Challenge", nach ISO 9798-2 gesendet. Die Antwort des Kontaktlos-Lesers ist bereits mit dem Authentisierungsschlüssel der Zielapplikation verschlüsselt. Ein Mechanismus, der sowohl in Hardware als auch in Software implementiert sein kann, überprüft alle virtuellen Karten auf Schlüsselübereinstimmung und selektiert im Erfolgsfall die übereinstimmende virtuelle Karte als aktive Karte. Beispielsweise kann nach ISO 9798-2 die Antwort der Karte berechnet werden und zum Kontaktlos-Leser gesendet werden, der die Applikationen dann weiterführt. In einem anderen Ausführungsbeispiel kann beispielsweise zunächst eine einzelne virtuelle Kartenanwendung herangezogen werden, wobei im erfolglosen Fall ein Indikator gespeichert wird, der diese Kartenanwendung für eine gewisse Zeit von einer Überprüfung ausschließt, um so sukzessive die richtige Kartenapplikation zu identifizieren.

[0035] Insbesondere wird darauf hingewiesen, dass abhängig von den Gegebenheiten Ausführungsbeispiele auch in Software implementiert sein können. Die Implementation kann auf einem digitalen Speichermedium, insbesondere einer Diskette, einer CD oder DVD mit elektronisch auslesbaren Steuersignalen erfolgen, die so mit einem programmierbaren Computersystem zusammenwirken, dass das entsprechende Verfahren ausgeführt wird. Allgemein können also Ausführungsbeispiele auch als Computerprogrammprodukt realisiert sein mit einem auf einem maschinenlesbaren Träger gespeicherten Programmcode zur Durchführung des entsprechenden Verfahrens, wenn das Computerprogrammprodukt auf einem Rechner abläuft. In anderen Worten ausgedrückt, können Ausführungsbeispiele somit als ein Computerprogramm mit einem Programmcode zur Durchführung des Verfahrens realisiert werden, wenn das Computerprogrammprodukt auf einem Computer abläuft.

[0036] Ausführungsbeispiele der Erfindung wurden oben anhand einer Multiapplikationskontaktloskarte oder eines NFC-tauglichen Gerätes (NFC = Near Field Communication) beschrieben. Die Erfindung ist nicht hierauf beschränkt. Ausführungsbeispiele der Erfindung können eine Anwendung eines multiapplikationstauglichen Geräts, z. B. einer über Kontakte lesbaren Karte, auswählen.

[0037] Ausführungsbeispiele der Erfindung betreffen das Zusammenspiel zwischen einer Karte und einem Lesegerät (Kartenleser). Die Erfindung ist jedoch nicht hierauf beschränkt. Weitere Ausführungsbeispiele der Erfindung betreffen die Auswahl einer Anwendung (Applikation) eines Geräts, z. B. eines NFC-Geräts, das mit einem Lesegerät, z. B. einem weiteren NFC-Gerät, kommuniziert. Das Gerät ist z. B. ein multiapplikationstaugliches Gerät, das mehrere Anwendungen (z. B. Kartenapplikationen) repräsentiert, die von einem Lesegerät, z. B. einem Kartenleser, bedient werden können.

Bezugszeichenliste

100	Vorrichtung zur Auswahl
110	Empfangseinrichtung
120	Überprüfungseinrichtung
130	Sendeeinrichtung
200	Selektionsschaltung
210	Empfänger
215	Empfangsantenne
218	Ausgang für Empfangssignal
220	Überprüfer
225	Eingang Überprüfer
228	Ausgang Überprüfer
229	Schnittstelle für mehrere Kartenanwendungen
230	Sender
235	Sendeantenne
238	Eingang für Sender
240	Multiapplikationscontrollerkarte
300	Selektionsschaltung
400	Flussdiagramm
410	Startpunkt
420	Antikollision und Selektion
430	Layer 4 Protokollauswahl
440	Konventionelle Auswahl
450	Ausführungsbeispiel

Patentansprüche

1. Vorrichtung (**100**) zur Auswahl einer Anwendung eines Geräts, mit folgenden Merkmalen:
einer Empfangseinrichtung (**110**) zum Empfangen eines Authentisierungskommandos, aus dem Informationen über einen Schlüssel eines Lesegeräts, das mit dem Gerät kommuniziert, ableitbar sind;
einer Überprüfungseinrichtung (**120**), um anhand der Informationen aus dem Authentisierungskommando solange zu überprüfen, ob eine der Anwendungen und das Lesegerät einen gemeinsamen Schlüssel verwenden, bis eine Schlüsselübereinstimmung gefunden ist oder alle Anwendungen überprüft sind und zur Selektion einer Anwendung für eine Kommunikation mit dem Lesegerät anhand der Schlüsselübereinstimmung, wobei die Überprüfungseinrichtung (**120**) ausgebildet ist, um zur Selektion der Anwendung die Anwendungen sequentiell zu überprüfen und Anwendungen mit einer erfolglosen Überprüfung temporär von der Überprüfung auszuschließen; und
einer Sendeeinrichtung (**130**) zum Senden einer Antwort der selektierten Anwendung an das Lesegerät.

2. Vorrichtung (**100**) gemäß Anspruch 1, bei der die Überprüfungseinrichtung (**120**) ferner eine Emulationseinrichtung zur Emulation der selektierten Anwendung und zum Generieren einer Antwort der selektierten Anwendung aufweist.

3. Vorrichtung (**100**) gemäß einem der Ansprüche 1 oder 2, die ferner eine Einrichtung zum Speichern der Anwendung aufweist.

4. Vorrichtung gemäß einem der Ansprüche 1 bis 3, die in einem portablen Gerät integriert ist.

5. Vorrichtung (**100**) gemäß Anspruch 4, die in einem Mobilfunktelefon, einem PDA oder einem portablen Computer implementiert ist.

6. Vorrichtung (**100**) gemäß einem der Ansprüche 1 bis 5, bei der die Überprüfungseinrichtung (**120**) ausgebildet ist, um zur Selektion der Anwendung die Anwendungen simultan zu überprüfen und diejenige Anwendung zu selektieren, die eine Schlüsselübereinstimmung liefert.

7. Vorrichtung (**100**) gemäß einem der Ansprüche 1 bis 6, bei der die Empfangseinrichtung (**110**) ausgebildet ist, um Signale gemäß zumindest einem der ISO 14443 Typ A, ISO 14443 Typ B, ISO 18092 oder ISO 15693 zu empfangen und die Sendeeinrichtung (**120**) ausgebildet ist, um Signale gemäß zumindest einem der ISO 14443 Typ A, ISO 14443 Typ B, ISO 18092 oder ISO 15693 zu senden.

8. Vorrichtung (**100**) gemäß einem der Ansprüche 1 bis 7, bei der Überprüfungseinrichtung (**120**) ausgebildet ist, um die Kartenanwendung gemäß einem Authentisierungsmechanismus gemäß ISO 9798-2-Standards zu überprüfen.

9. Vorrichtung (**100**) zur Auswahl einer Anwendung eines Geräts, mit folgenden Merkmalen:
einer Empfangseinrichtung (**110**) zum Empfangen eines Authentisierungskommandos, aus dem Informationen über einen Schlüssel eines Lesegeräts, das mit dem Gerät kommuniziert, ableitbar sind;
einer Überprüfungseinrichtung (**120**), um anhand der Informationen aus dem Authentisierungskommando

zu überprüfen, ob eine der Anwendungen und das Lesegerät einen gemeinsamen Schlüssel verwenden, wobei im erfolgslosen Fall diese Anwendung für eine gewisse Zeit von der Überprüfung ausgeschlossen wird, um so sukzessive die richtige Anwendung zu finden und zur Selektion einer Anwendung für eine Kommunikation mit dem Lesegerät anhand einer Schlüsselübereinstimmung; und
einer Sendeeinrichtung (**130**) zum Senden einer Antwort der selektierten Anwendung an das Lesegerät.

10. Vorrichtung (**100**) gemäß Anspruch 9, bei der die Überprüfungseinrichtung (**120**) ferner eine Emulationseinrichtung zur Emulation der selektierten Anwendung und zum Generieren einer Antwort der selektierten Anwendung aufweist.

11. Vorrichtung (**100**) gemäß einem der Ansprüche 9 oder 10, bei der die Überprüfungseinrichtung (**220**) mit einem multiapplikationstauglichen Gerät gekoppelt ist.

12. Vorrichtung (**100**) gemäß einem der Ansprüche 9 bis 11, die ferner eine Einrichtung zum Speichern der Anwendung aufweist.

13. Vorrichtung (**100**) gemäß einem der Ansprüche 9 bis 12, die in einem portablen Gerät integriert ist.

14. Vorrichtung (**100**) gemäß Anspruch 13, die in einem Mobilfunktelefon, einem PDA oder einem portablen Computer implementiert ist.

15. Vorrichtung (**100**) gemäß einem der Ansprüche 9 bis 14, die ferner einen Emulator zur Emulation einer virtuellen Anwendung aufweist.

16. Vorrichtung (**100**) gemäß einem der Ansprüche 9 bis 15, bei der die Empfangseinrichtung (**110**) ausgebildet ist, um das Authentisierungskommando aus einem Empfangssignal gemäß zumindest einem der ISO 14443 Typ A, ISO 14443 Typ B, ISO 18092 oder ISO 15693 bereitzustellen.

17. Vorrichtung (**100**) gemäß einem der Ansprüche 9 bis 16, bei der die Sendeeinrichtung (**130**) zum Senden der Antwort der selektierten Anwendung ausgebildet ist, um ein Antwortsignal gemäß zumindest einem der ISO 14443 Typ A, ISO 14443 Typ B, ISO 18092 oder ISO 15693 bereitzustellen.

18. Selektionsschaltung (**200**; **300**) mit
einem Empfänger (**210**) mit einem Ausgang (**218**) an dem ein Empfangssignal empfangbar ist, aus dem Informationen über einen Authentisierungsschlüssel ableitbar sind;
einem Überprüfer (**220**) mit einem Eingang (**225**) der mit dem Ausgang (**218**) des Empfängers (**210**) gekoppelt ist, einer Schnittstelle (**229**) für mehrere virtuelle Anwendungen, über die der Authentisierungsschlüssel anhand der Informationen aus dem Empfangssignal solange verifizierbar ist, bis eine Authentisierungsschlüsselübereinstimmung mit einer virtuellen Anwendung gefunden ist oder alle virtuellen Anwendungen überprüft sind, wobei durch den Überprüfer (**220**) ferner zur Verifikation des Authentisierungsschlüssels Indikatoren für Anwendungen mit fehlgeschlagenen Verifikationen temporär speicherbar sind, und einem Ausgang (**228**) für ein Antwortsignal der virtuellen Anwendung, für die der Authentisierungsschlüssel verifizierbar ist;
einem multiapplikationstauglichen Gerät (**240**), das mit der Schnittstelle (**229**) für mehrere virtuelle Anwendungen gekoppelt ist und einen Speicher umfasst, der wenigstens zwei virtuelle Anwendungen speichert; und
einem Sender (**230**) mit einem Eingang (**238**), der mit dem Ausgang (**228**) für das Antwortsignal gekoppelt ist.

19. Selektionsschaltung (**200**; **300**) gemäß Anspruch 18, bei der der Überprüfer (**220**) einen Emulator umfasst, der das Antwortsignal durch Emulation der virtuellen Anwendung, für die der Authentisierungsschlüssel verifizierbar ist, bereitstellt.

20. Selektionsschaltung (**200**; **300**) gemäß einem der Ansprüche 18 oder 19, bei der das multiapplikationstaugliche Gerät (**240**) virtuelle Anwendungen der gleichen Art oder in der gleichen Kommunikationstechnologie speichert.

21. Selektionsschaltung (**200**; **300**) gemäß einem der Ansprüche 18 bis 20, bei der der Überprüfer (**220**) ausgebildet ist, um den Authentisierungsschlüssel unter Verwendung eines Protokolls zu verifizieren.

22. Selektionsschaltung (**200**; **300**) gemäß Anspruch 21, wobei das Protokoll einem der Mifare Classic, oder My-D Standards entspricht.

23. Selektionsschaltung (**200**; **300**) gemäß einem der Ansprüche 18 bis 22, bei der der Empfänger (**210**) und der Sender (**230**) ausgebildet sind, um gemäß zumindest einen der ISO 14443 Typ A, ISO 14443 Typ B, ISO 18092 oder ISO 15693 zu kommunizieren.

24. Selektionsschaltung (**200**; **300**) gemäß einem der Ansprüche 18 bis 23, bei der der Authentisierungsschlüssel durch den Überprüfer (**220**) gemäß des ISO 9798-2 Standards verifizierbar ist.

25. Verfahren zur Auswahl einer Anwendung aus einer Mehrzahl von Anwendungen eines Geräts, mit folgenden Schritten:
Empfangen eines Authentisierungskommandos, aus dem Informationen über einen Schlüssel eines Lesegeräts, das mit dem Gerät kommuniziert, ableitbar

sind;
anhand der Informationen aus dem Authentisierungskommando, solange Überprüfen ob eine der Anwendungen und das Lesegerät einen gemeinsamen Schlüssel verwenden bis eine Schlüsselübereinstimmung gefunden ist oder alle Anwendungen überprüft sind, wobei Anwendungen nach einer erfolglosen Überprüfung temporär von dem Überprüfen ausgeschlossen werden;
Selektion der Anwendung für die das Überprüfen erfolgreich war; und
Antworten gemäß der selektierten Anwendung.

26. Verfahren gemäß Anspruch 25, bei dem der Schritt des Selektierens ferner einen Schritt des Emulierens der selektierten Anwendung umfasst.

27. Verfahren gemäß einem der Ansprüche 25 oder 26, das vor dem Schritt des Empfangens einen Schritt des Speicherns der Mehrzahl von Anwendung umfasst.

28. Verfahren gemäß einem der Ansprüche 25 bis 27, bei dem der Schritt des Überprüfens Unterschritte des sequentiellen Überprüfens der einzelnen Anwendung der Mehrzahl von Anwendung umfasst.

29. Verfahren gemäß einem der Ansprüche 25 bis 28, bei dem der Schritt des Überprüfens einen Schritt des simultanen Überprüfens von wenigstens zwei Anwendungen der Mehrzahl von Anwendungen umfasst.

30. Verfahren gemäß einem der Ansprüche 25 bis 29, bei dem der Schritt des Empfangens ferner das Empfangen von Signalen gemäß zumindest einem der ISO 14443 Typ A, ISO 14443 Typ B, ISO 18092, ISO 15693, Mifare Classic, oder My-D Standards umfasst und der Schritt des Antwortens das Senden eines Signals gemäß einem dieser Standards umfasst.

31. Verfahren gemäß einem der Ansprüche 25 bis 30, bei dem der Schritt des Überprüfens das Überprüfen gemäß ISO 9798-2 umfasst.

32. Computerprogramm mit einem Programmcode zur Durchführung eines der Verfahren gemäß einem der Ansprüche 25 bis 31, wenn der Programmcode auf einem Computer abläuft.

33. Verfahren zur Selektion einer virtuellen Kartenanwendung auf einer Multiapplikationscontrollerkarte, die wenigstens zwei virtuelle Kartenanwendungen bereitstellt, mit folgenden Schritten:
Empfangen Informationen über einen Schlüssel eines Kartenlesers ableitbar sind;
Überprüfen an wenigstens zwei virtuellen Kartenanwendungen, ob eine der virtuellen Kartenanwendungen und der Kartenleser einen gemeinsamen Schlüssel verwenden solange bis eine Schlüsselübereinstimmung gefunden ist oder alle virtuellen Anwendungen überprüft sind, wobei Anwendungen nach einer erfolglosen Überprüfung temporär von dem Überprüfen ausgeschlossen werden;
Identifikation einer Schlüsselübereinstimmung mit einer passenden Kartenanwendung der wenigstens zwei virtuellen Kartenanwendungen;
Emulation der passenden Kartenanwendungen;
Antworten an den Kartenleser gemäß des Protokolls und der passenden Kartenanwendung.

34. Verfahren gemäß Anspruch 33, bei dem der Schritt des Überprüfens eine 3-Pass-Authentication gemäß ISO 9798-2 umfasst.

35. Verfahren gemäß einem der Ansprüche 33 oder 34, bei dem das Protokoll zumindest einem der ISO 14443 Typ A, ISO 14443 Typ B, ISO 18092, ISO 1593, Mifare Classic oder My-D entspricht.

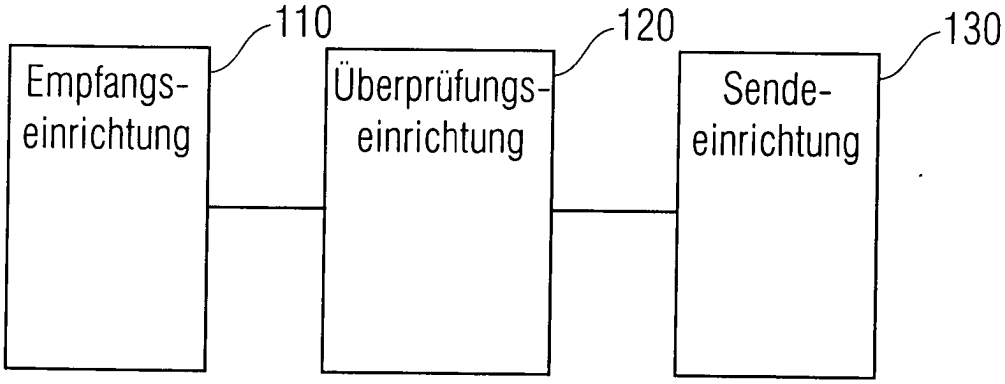
36. Verfahren gemäß einem der Ansprüche 33 bis 35, das ferner einen Schritt des Speicherns der wenigstens zwei virtuellen Kartenanwendungen umfasst.

37. Computerprogramm mit einem Programmcode zur Durchführung eines der Verfahren gemäß einem der Ansprüche 33 bis 36, wenn der Programmcode auf einem Computer ausgeführt wird.

Es folgen 3 Blatt Zeichnungen

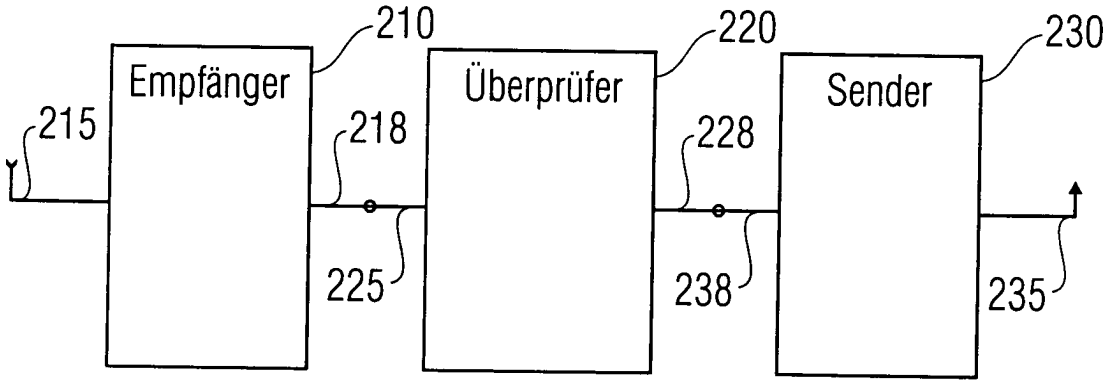
Anhängende Zeichnungen

FIG 1



100

FIG 2a



200

FIG 2b

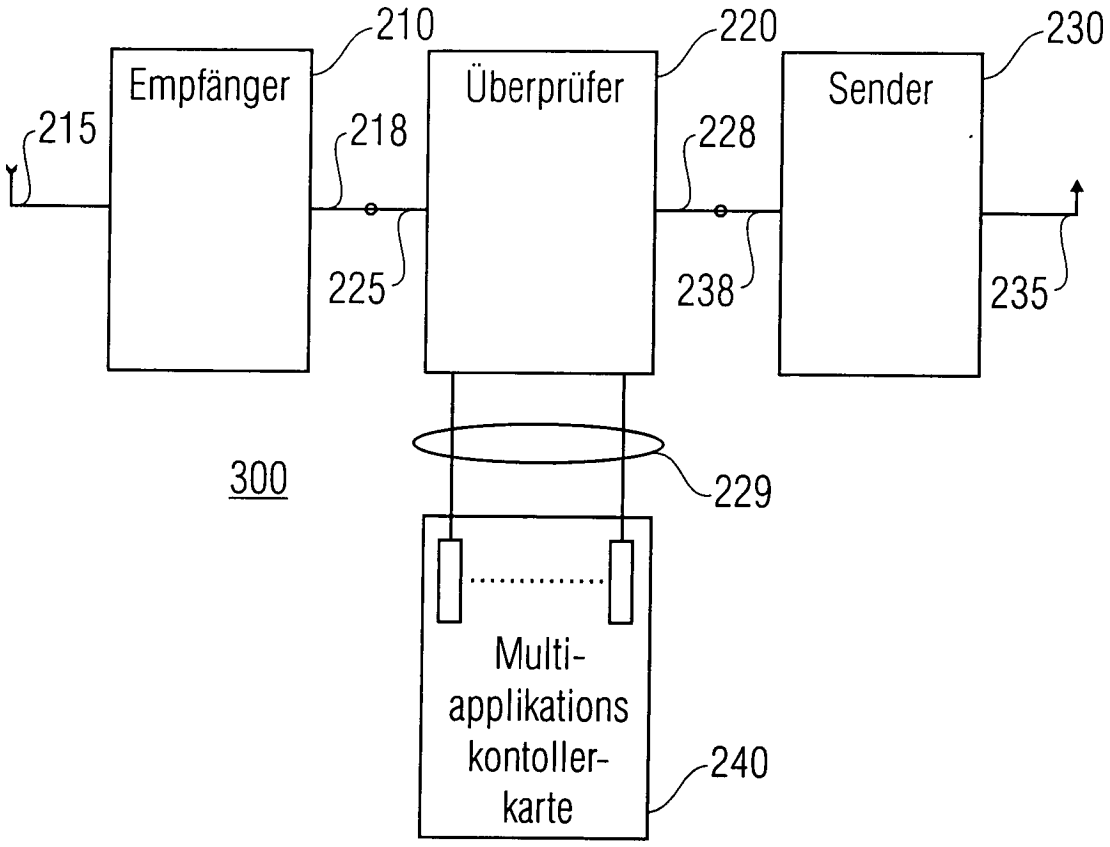
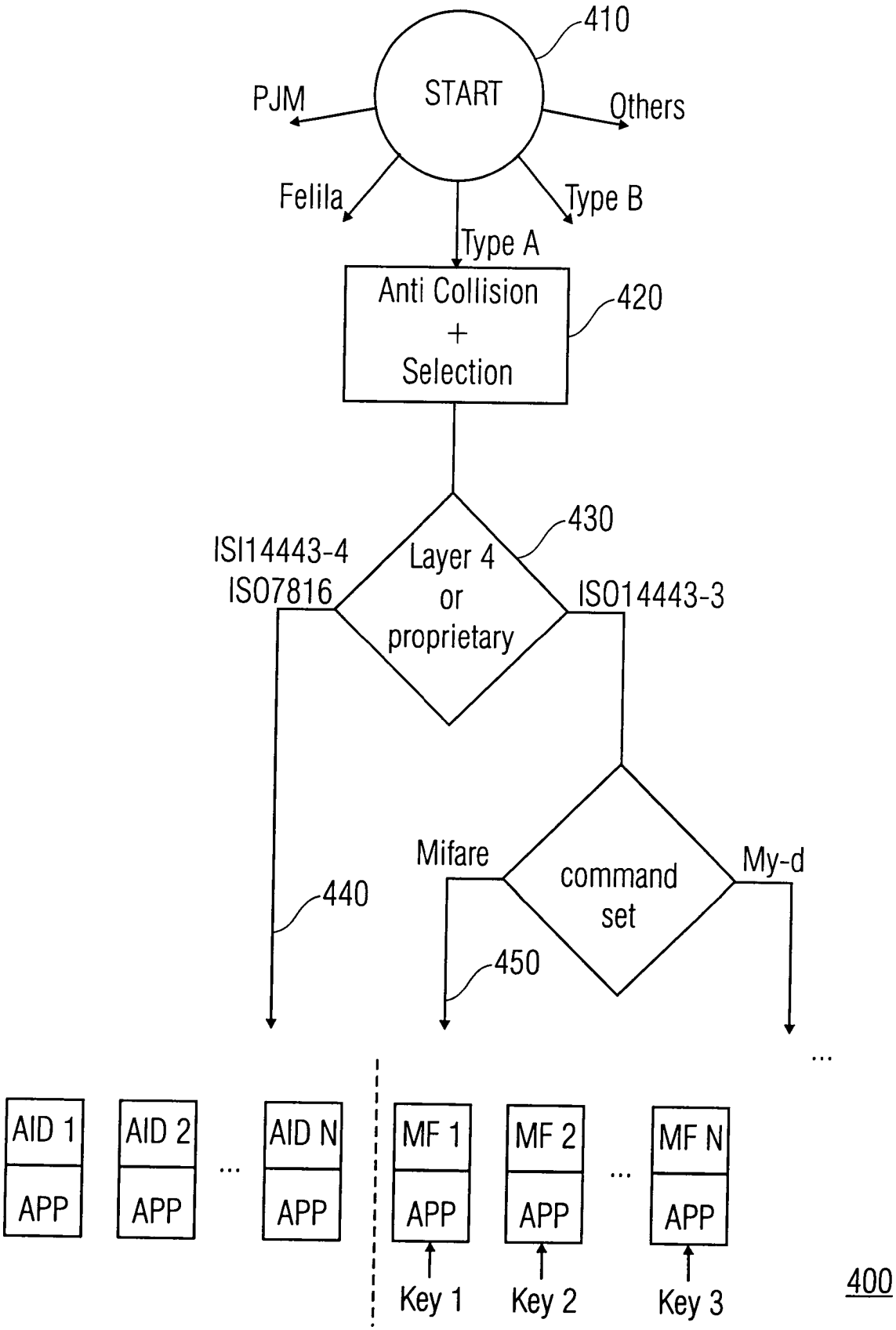

210
220
230
Empfänger
Überprüfer
Sender
215
218
228
225
238
235
300
229
Multi-
applikations
kontoller-
karte
240

FIG 3


410
START
PJM
Others
Felila
Type B
Type A
Anti Collision
+
Selection
420
430
ISI14443-4
ISO7816
Layer 4
or
proprietary
ISO14443-3
Mifare
command
set
My-d
440
450
...
AID 1
APP
AID 2
APP
...
AID N
APP
MF 1
APP
MF 2
APP
...
MF N
APP
Key 1
Key 2
Key 3
400