(19) Deutsches Patent- und Markenamt

(10) **DE 10 2011 078 121 A1** 2012.12.27

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2011 078 121.8**
(22) Anmeldetag: **27.06.2011**
(43) Offenlegungstag: **27.12.2012**

(51) Int Cl.: ***G06F 3/033*** (2011.01)

(71) Anmelder:
Bundesdruckerei GmbH, 10969, Berlin, DE

(74) Vertreter:
RICHARDT PATENTANWÄLTE GbR, 65185, Wiesbaden, DE

(72) Erfinder:
Herrmann, Klaus, Dr., 30625, Hannover, DE; Schubert, Michael, 30419, Hannover, DE; Wolf, Andreas, Dr., 07743, Jena, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:

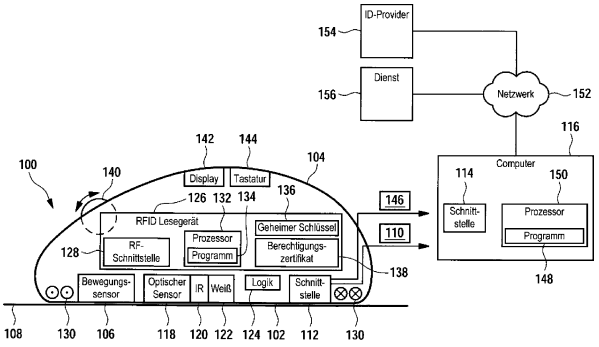
DE 10 2007 000 885 A1
US 2006 / 0 007 151 A1

Prüfungsantrag gemäß § 44 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Computermaus und Verfahren zum Lesen von Daten aus einem Dokument**

(57) Zusammenfassung: Die Erfindung betrifft eine Computermaus mit zumindest einem ersten an der Unterseite (102) der Computermaus angeordneten optischen Sensor (118), der zum Einscannen zumindest eines Teilbereichs (202) eines Dokuments (200) ausgebildet ist, und mit einer RF-Schnittstelle (128) für eine drahtlose Kommunikation mit einem RFID-Chip (206) des Dokuments, wobei die Computermaus einen ersten Betriebsmodus zur Erfassung einer Position oder Bewegung der Computermaus relativ zu einer Unterlage und einem zweiten Betriebsmodus zur Durchführung eines Lesezugriffs auf den RFID-Chip des Dokuments aufweist, wobei die Computermaus für das Einscannen des Teilbereichs in dem zweiten Betriebsmodus zur Ermöglichung einer Berechtigungsprüfung für den Lesezugriff ausgebildet ist, und mit Prozessormitteln (132, 134) zur Ausführung von Schritten eines kryptographischen Protokolls für die Durchführung der Berechtigungsprüfung.



Beschreibung

[0001] Die Erfindung betrifft eine Computermaus, ein elektronisches System sowie ein Verfahren zum Lesen von Daten aus einem Dokument.

[0002] Bei einer Computermaus handelt es sich um ein Manipulandum, welches dazu dient, um von einem Benutzer über eine Unterlage bewegt zu werden. Durch die Computermaus wird diese Bewegung sensiert und durch ein Computersystem, an welches die Computermaus angeschlossen ist, zum Beispiel in die Bewegung eines Cursors einer graphischen Nutzeroberfläche des Computersystems umgesetzt. Aus DE 198 58 935 A1, DE 102 60 924 B3, DE 10 2004 023 845 A1 und EP 2 254 325 A1 sind verschiedene Ausführungsformen solcher Computermäuse bekannt.

[0003] Der Erfindung liegt demgegenüber die Aufgabe zugrunde, eine verbesserte Computermaus zu schaffen, sowie ein elektronisches System und ein Verfahren zum Lesen von Daten aus einem Dokument.

[0004] Die der Erfindung zugrunde liegende Aufgabe wird jeweils mit den Merkmalen der unabhängigen Patentansprüche gelöst. Ausführungsformen der Erfindung sind in den abhängigen Patentansprüchen angegeben.

[0005] Der Begriff „Computermaus" schließt erfindungsgemäß jedes von einem Benutzer betätigbare Manipulandum ein, welches zur Sensierung einer Position oder einer Bewegung der Computermaus auf einer Unterlage ausgebildet ist. Der Positions- oder Bewegungssensor der Computermaus kann dabei mechanisch oder optisch ausgebildet sein; im letzteren Fall spricht man von einer „optischen Maus". Die Computermaus kann drahtgebunden oder drahtlos mit dem Computersystem kommunizieren und von dem Computersystem mit elektrischer Energie versorgt werden oder eine eigene Energieversorgung, insbesondere eine Batterie, aufweisen. Im Sinne der vorliegenden Erfindung wird unter einer Computermaus auch ein computermausförmiges Gerät verstanden, welches zum Beispiel einen sogenannten Trackball aufweist, um den Cursor zu steuern; in diesem Fall erfolgt die Steuerung des Cursors also nicht durch Bewegung der Computermaus, sondern durch Bewegung eines Teils der Computermaus, beispielsweise also durch Drehung des Trackballs.

[0006] Unter einem „Dokument" wird hier jedes Dokument verstanden, welches einen Chip, d. h eine integrierte elektronische Schaltung, beinhaltet, wobei das Dokument zum Beispiel Kunststoff- und/oder Papier-basiert sein kann. Bei dem Dokument kann es sich um ein Wert- oder Sicherheitsdokument, wie zum Beispiel um ein ID-Dokument, d. h. ein Ausweisdokument, wie zum Beispiel einen Personalausweis, Reisepass, Führerschein, Fahrzeugbrief, Fahrzeugschein oder Firmenausweis, oder ein Zahlungsmittel, wie zum Beispiel eine Banknote, eine Kreditkarte oder einen sonstigen Berechtigungsnachweis, wie zum Beispiel eine Eintrittskarte, einen Frachtbrief, ein Visum oder dergleichen, handeln. Insbesondere kann es sich beim Dokument um eine Chipkarte handeln. Unter einem Dokument wird hier auch ein Dokument verstanden, welches buchartig ausgebildet ist, wie dies zum Beispiel bei einem Reisepass der Fall ist.

[0007] Der Chip des Dokuments ist als RFID-Chip ausgebildet. Unter einem „RFID-Chip" wird hier jeder Chip verstanden, welcher zur Ausführung eines RFID oder Near Field Communication(NFC)-Übertragungsverfahren ausgebildet ist, insbesondere nach dem Standard ISO14443.

[0008] Beispielsweise hat das Dokument einen Dokumentenkörper mit einer integrierten Antenne, wie zum Beispiel ein oder mehrere Antennenwicklungen, die am Rand des Dokumentenkörpers verlaufen, wobei die Antenne an den RFID-Chip angeschlossen ist. Beispielsweise kann es sich bei einem solchen Dokument um einen elektronischen Reisepass oder einen elektronischen Personalausweis handeln.

[0009] Das Dokument hat zumindest einen Teilbereich, der eine Information trägt, die zum optischen Einscannen vorgesehen ist; bei diesem Teilbereich kann es sich um die sogenannte Machine Readable Zone (MRZ) und/oder die Card Access Number (CAN) eines maschinenlesbaren Reisedokuments (Machine Readable Travel Document – MRTD) handeln. Die Information kann mit einer speziellen Druckfarbe auf den Teilbereich aufgedruckt sein, welche sich zur optischen Sensierung im Infrarotbereich eignet.

[0010] Das Dokument kann optische Sicherheitsmerkmale, wie zum Beispiel ein aufgedrucktes oder auf einem Display des Dokuments angezeigtes Passbild, ein Wappen, Siegel oder andere Merkmale des Sicherheitsdrucks aufweisen.

[0011] Ausführungsformen der erfindungsgemäßen Computermaus sind besonders vorteilhaft, da die Computermaus in ihrem ersten Betriebsmodus wie eine übliche Computermaus zum Beispiel zur Steuerung der Position eines Cursors auf einer graphischen Benutzeroberfläche verwendet werden kann, während die Computermaus in ihrem zweiten Betriebsmodus die Funktion eines RFID-Lesegeräts zum Lesen von Daten aus dem RFID-Chip eines Dokuments wahrnimmt, indem die Computermaus statt auf einer Unterlage auf einem Dokument positioniert und/oder bewegt wird.

[0012] Zur Integration der Funktion eines RFID-Lesegeräts zum Lesen beispielsweise des elektronischen Reisepasses oder des elektronischen Personalausweises und der Ausführung der hierzu erforderlichen kryptographischen Protokolle hat die Computermaus einen optischen Sensor zum Einscannen des Teilbereichs des Dokuments, beispielsweise also der MRZ oder der CAN. Hierdurch kann eine Information erfasst werden, die für die Durchführung des kryptographischen Protokolls erforderlich ist, beispielsweise des Basic Access Control (BAC) und/oder Extended Access Control (EAC) Protocols, wie es von der Internationalen Luftfahrtbehörde (ICAO) spezifiziert ist, und/oder des Password Authenticated Connection Establishment(PACE)-Protokolls, vergleiche hierzu Bundesamt für Sicherheit in der Informationstechnik (BSI, Technical Guideline TR-03110 sowie EP 1 891 607 B1).

[0013] Nach Ausführungsformen der Erfindung hat die Computermaus zumindest einen Mikroprozessor zur Ausführung von Programminstruktionen, welche diejenigen Schritte eines kryptographischen Protokolls implementieren, welche seitens des in die Computermaus integrierten RFID-Lesegeräts erforderlich sind, um lesend auf die in dem RFID-Chip des Dokuments gespeicherten Daten zuzugreifen. Die von dem Teilbereich des Dokuments durch Einscannen optisch erfasste Information geht in diesen kryptographischen Algorithmus zur Ermöglichung einer Berechtigungsprüfung für den lesenden Zugriff auf die Daten ein.

[0014] Zur Durchführung des kryptographischen Protokolls werden zwischen dem Prozessor der Computermaus und dem RFID-Chip des Dokuments über eine Radiofrequenz zum Beispiel mit einem Request/Response-Protokoll Daten ausgetauscht, insbesondere in sogenannten Application Data Units (APDUs), und zwar über die RF-Schnittstelle der Computermaus, an welche der Prozessor angeschlossen ist.

[0015] Ausführungsformen der Erfindung sind besonders vorteilhaft, da durch die Integration der Funktionalität eines RFID-Lesegeräts in eine Computermaus ein separates RFID-Lesegerät an dem Computerarbeitsplatz eines Benutzers entfallen kann. Dies hat einerseits Kostenvorteile, da ohnehin vorhandene Komponenten der Computermaus für die Integration der RFID-Funktionalität verwendet werden können, und hat andererseits Handhabungsvorteile sowie Sicherheitsvorteile für den Benutzer.

[0016] Insbesondere wird durch die Integration des Lesegeräts in die Computermaus sichergestellt, dass das Dokument nicht länger als notwendig im Erfassungsbereich des Lesegeräts bleibt, was bei einem separaten Lesegerät nicht der Fall ist. Wenn der Benutzer nämlich nach der Durchführung des Lesezugriffs weiter arbeiten möchte, so muss wieder in den ersten Betriebsmodus der Computermaus zurückgegangen werden, in dem kein Zugriff auf das Dokument möglich ist, da das in die Computermaus integrierte Lesegerät dann deaktiviert ist. Dies minimiert das Risiko, dass über zum Beispiel auf dem Computer installierte Malware der Versuch unternommen, über das Lesegerät einen unerlaubten Zugriff auf das Dokument durchzuführen, da nach dem Lesezugriff das in die Computermaus integrierte RFID Lesegerät deaktiviert und das Dokument aus dessen Erfassungsbereich zwangsläufig entfernt wird, um die Computermaus in dem ersten Betriebsmodus zu verwenden.

[0017] Nach einer Ausführungsform ist an der Unterseite der Computermaus eine Infrarotstrahlungsquelle angeordnet, die in dem zweiten Betriebsmodus eingeschaltet ist, wobei der erste optische Sensor der Computermaus in einem Infrarotspektralbereich strahlungssensitiv ist. Beispielsweise wird eine Infrarotstrahlungsquelle im Bereich 850–900 nm eingesetzt. Dies vereinfacht die Erfassung der Information von dem Teilbereich des Dokuments, wenn dieser mit einer speziellen Druckfarbe aufgedruckt ist, die im Infrarotbereich sichtbar ist.

[0018] Nach einer Ausführungsform der Erfindung ist an der Unterseite der Computermaus eine weitere Strahlungsquelle angeordnet, die Licht in einem sichtbaren Spektralbereich abgibt, insbesondere eine Weißlichtstrahlungsquelle. Der erste optische Sensor ist zusätzlich in diesem sichtbaren Spektralbereich sensitiv, um so die Erfassung eines oder mehrerer optischer Sicherheitsmerkmale des Dokuments zu ermöglichen. Der erste optische Sensor kann beispielsweise als Kamera mit einem Objektiv ausgebildet sein. Beispielsweise kann ein Kameratyp zum Einsatz kommen, wie er auch in sogenannten Webcams verwendet wird.

[0019] Nach einer Ausführungsform der Erfindung wird der erste optische Sensor sowohl in dem ersten Betriebsmodus als auch in dem zweiten Betriebsmodus verwendet: in dem ersten Betriebsmodus wird der erste optische Sensor als Positions- oder Bewegungssensor eingesetzt, wie das bei einer optischen Computermaus üblicherweise der Fall ist. Dagegen wird der erste optische Sensor in dem zweiten Betriebsmodus zum Einscannen des Teilbereichs des Dokuments für die Erfassung der Information verwendet. Hierdurch ist ein Kostenvorteil gegeben, da kein zusätzlicher optischer Sensor für den zweiten Betriebsmodus erforderlich ist. Es kann aber auch ein zusätzlicher zweiter optischer oder mechanischer Sensor vorgesehen sein, der in dem ersten Betriebsmodus als Positions- oder Bewegungssensor wirkt, während der erste optische Sensor dann inaktiv ist.

[0020] Nach einer Ausführungsform der Erfindung ist in die Computermaus eine Antenne integriert, die ein oder mehrere Antennenwicklungen aufweist. Die Öffnung der dadurch gebildeten Antennenspule ist auf die Unterseite der Computermaus ausgerichtet; beispielsweise liegen die Antennenwicklungen auf oder in der Unterseite des Gehäuses der Computermaus zur Realisierung eines hohen Kopplungsfaktors mit einem an der Unterseite der Computermaus anliegenden Dokument.

[0021] Nach einer Ausführungsform der Erfindung hat die Computermaus Eingabemittel zur Eingabe einer Kennung, insbesondere einer Personal Identification Number (PIN). Als Eingabemittel kann zum Beispiel eine Tastatur vorgesehen sein, die insbesondere in einem Rückenbereich der Computermaus angeordnet sein kann. Zusätzlich kann auch eine Anzeigevorrichtung, wie zum Beispiel ein LCD-Display, in die Computermaus integriert sein, zum Beispiel ebenfalls in deren Rückenbereich, um so zum Beispiel ein Klasse 2- oder Klasse 3-Lesegerät zu verwirklichen.

[0022] Die Eingabe der Kennung kann erforderlich sein, um das Dokument zur Freigabe einer Chipkartenfunktion freizuschalten und/oder im Rahmen einer Authentifizierung des Benutzers gegenüber dem Dokument. Alternativ oder zusätzlich zu der Kennung kann die Erfassung eines biometrischen Merkmals von dem Benutzer für die Nutzer-Authentifizierung erforderlich sein, wozu ein entsprechender Biometriesensor in die Computermaus integriert sein kann.

[0023] Nach einer Ausführungsform der Erfindung hat die Computermaus ein Bedienelement, wie zum Beispiel einen Bedienknopf, zur Wahl des ersten oder des zweiten Betriebsmodus. Diese Umschaltfunktion kann vollständig in der Computermaus selbst implementiert sein oder über ein Anwendungsprogramm des Computers erfolgen.

[0024] Nach einer Ausführungsform der Erfindung hat die Computermaus Zugriffsmittel zum Zugriff auf ein Berechtigungszertifikat der Computermaus.

[0025] Unter einem „Zertifikat" wird hier ein digitales Zertifikat verstanden, welches auch als Public-Key-Zertifikat bezeichnet wird. Bei einem Zertifikat handelt es sich um strukturierte Daten, die dazu dienen, einen öffentlichen Schlüssel eines asymmetrischen Kryptosystems einer Identität, wie zum Beispiel einer Person oder einer Vorrichtung, hier also der Computermaus oder einem ID-Provider-Computersystem, zuzuordnen. Beispielsweise kann das Zertifikat dem Standard X.509 oder einem anderen Standard entsprechen.

[0026] Unter einem „Berechtigungszertifikat" wird hier ein Zertifikat verstanden, welches eine zusätzliche Angabe des Umfangs einer Zugriffsberechtigung auf die in dem Dokument gespeicherten Daten angibt, also beispielsweise spezifiziert, auf welche der in dem Dokument gespeicherten Datengruppen lesend zugegriffen werden darf.

[0027] Das Berechtigungszertifikat kann lokal in einem elektronischen Speicher der Computermaus gespeichert sein. Alternativ kann das Berechtigungszertifikat an einer anderen Stelle gespeichert sein, wie zum Beispiel auf einem externen Servercomputer oder einem separaten ID-Token, wie zum Beispiel einer Chipkarte, welche einem berechtigten Nutzer zugeordnet ist. Im letzteren Fall ist die für den Zugriff berechtigte Entität also nicht unmittelbar die Computermaus, sondern ein berechtigter Benutzer, der diese Berechtigung zum Beispiel mit Hilfe einer entsprechenden Chipkarte nachweisen muss. Zu diesem Zweck kann in der Computermaus ein Chipkartenlesegerät implementiert sein, so dass die Computermaus auf ein in einer Chipkarte gespeichertes Berechtigungszertifikat zugreifen kann.

[0028] Nach einer Ausführungsform der Erfindung sind die in dem RFID Chip des Dokuments gespeicherten Daten, insbesondere zumindest ein Datenobjekt, digital signiert. Beim Lesen der Daten wird diese Signatur geprüft, beispielsweise mittels sogenannter Passive Authentication (PA), vgl. hierzu ebenfalls TR-03110.

[0029] In einem weiteren Aspekt betrifft die Erfindung ein elektronisches System mit zumindest einem Computer, wie zum Beispiel einem PC, und einer daran angeschlossenen erfindungsgemäßen Computermaus.

[0030] In einem weiteren Aspekt betrifft die Erfindung ein Verfahren zum Lesen von Daten aus einem Dokument mit Hilfe eines solchen elektronischen Systems.

[0031] Im Weiteren werden Ausführungsformen der Erfindung mit Bezugnahme auf die Zeichnungen näher erläutert. Es zeigen:

[0032] Fig. 1 ein Blockdiagramm zur Darstellung von Ausführungsformen einer erfindungsgemäßen Computermaus und eines erfindungsgemäßen elektronischen Systems,

[0033] Fig. 2 ein Blockdiagramm einer Ausführungsform eines Dokuments des elektronischen Systems,

[0034] Fig. 3 ein Blockdiagramm einer Ausführungsform eines erfindungsgemäßen Verfahrens,

[0035] Fig. 4 eine perspektivische Ansicht einer Ausführungsform einer erfindungsgemäßen Computermaus,

[0036] Fig. 5 eine Draufsicht auf eine Ausführungsform einer erfindungsgemäßen Computermaus mit einem Trackball.

[0037] Elemente der nachfolgenden Ausführungsformen, die einander entsprechen, sind mit identischen Bezugszeichen gekennzeichnet.

[0038] Die Fig. 1 zeigt eine Computermaus **100** mit einem Gehäuse, das eine flache Unterseite **102** und eine bogenförmig gewölbte Oberseite **104** aufweist. Die Computermaus **100** hat einen Bewegungssensor **106**, welcher mechanisch oder optisch ausgebildet sein kann. Bei einer Bewegung der Computermaus **100** über eine Unterlage **108** gibt der Bewegungssensor Signale **110** ab, die eine Relativbewegung der Computermaus **100** zu der Unterlage **108** anzeigen, und welche von einer Schnittstelle **112** der Computermaus **100** an eine entsprechende Schnittstelle **114** eines Computers **116**, zum Beispiel eines PCs, übertragen werden. Die Schnittstelle **112** kann kontaktbehaftet, zum Beispiel als USB-Schnittstelle, oder für eine kontaktlose Übertragung an die Schnittstelle **114** ausgebildet sein.

[0039] Die Computermaus **100** hat einen optischen Sensor **118**, der zum Einscannen zumindest eines Teilbereichs **202** eines Dokuments **200** (vergleiche Fig. 2) ausgebildet ist. Beispielsweise kann der optische Sensor **118** eine Kamera mit einem Objekt aufweisen. Der optische Sensor **118** kann so ausgebildet sein, dass er sowohl in einem sichtbaren Spektralbereich als auch in einem nicht-sichtbaren Spektralbereich, insbesondere in einem Infrarotbereich, sensitiv ist. Die Computermaus **100** kann dementsprechend eine Strahlungsquelle **120** für Infrarot(IR)-Strahlung und eine Strahlungsquelle **122** für Strahlung in einem sichtbaren Spektralbereich, insbesondere eine Weißlichtquelle, aufweisen. Dies ist vorteilhaft, um nacheinander eine Information von dem Teilbereich des Dokuments mit Hilfe der IR-Strahlungsquelle **120** zu erfassen und ein oder mehrere optische Sicherheitsmerkmale des Dokuments mit Hilfe der Strahlungsquelle **122** zu erfassen, um diese überprüfen zu können.

[0040] Die Computermaus **100** hat einen ersten Betriebsmodus, in dem der Bewegungssensor **106** aktiviert ist, um eine Bewegung der Computermaus zu erfassen, so dass die Signale **110** gesendet werden, und einen zweiten Betriebsmodus, in dem der optische Sensor **118** aktiv ist, um den Teilbereich des Dokuments einzuscannen sowie – je nach Ausführungsform – optische Sicherheitsmerkmale von dem Dokument zu erfassen.

[0041] Anstelle dessen kann auf den Bewegungssensor **106** verzichtet werden, wenn der optische Sensor **118** in dem ersten Betriebsmodus als optischer Bewegungssensor fungiert, wie das an sich für optische Computermäuse bekannt ist.

[0042] Zum Umschalten zwischen dem ersten Betriebsmodus und dem zweiten Betriebsmodus sowie für die entsprechende Aktivierung bzw. Deaktivierung der Komponenten der Computermaus je nach dem gewählten Betriebsmodus kann die Computermaus **100** eine Logikkomponente **124** aufweisen, wie zum Beispiel eine festverdrahtete Logikschaltung oder einen Mikrocontroller.

[0043] Die Computermaus **100** beinhaltet ein integriertes RFID-Lesegerät **126** zum Lesen von Daten aus dem Dokument **200**. Das RFID-Lesegerät **126** hat eine Radiofrequenz (RF) Schnittstelle **128** zur Durchführung eines RFID- oder NFC-Übertragungsverfahrens, welche an einer Antenne angeschlossen ist, die ein oder mehrere Antennenwicklungen **130** aufweist, durch welche eine Antennenspule gebildet wird.

[0044] In der hier betrachteten Ausführungsform sind die Antennenwicklungen **130** nebeneinander auf der Unterseite **102** im inneren des Gehäuses der Computermaus **100** angeordnet. Alternativ können die Antennenwicklungen **130** auch in der die Unterseite **102** bildenden Gehäusewandung oder auf der äußeren Oberfläche der Unterseite **102** angeordnet sein, um einen möglichst hohen Kopplungsfaktor zu erreichen. Vorzugsweise ist die Antennenspule koplanar zu der Unterseite **102** sowie der Unterlage **108** angeordnet, so dass die Öffnung der Antennenspule nach unten ausgerichtet ist, wie in der Fig. 1 gezeigt.

[0045] Das RFID-Lesegeräte **126** beinhaltet zumindest einen Prozessor **132** zur Ausführung von Programminstruktionen **134** sowie zumindest einen elektronischen Speicher mit einem geschützten Speicherbereich **136** zur Speicherung eines geheimen Schlüssels und einem Speicherbereich **138** zur Speicherung eines dem geheimen Schlüssel zugeordneten Berechtigungszertifikats.

[0046] Alternativ können der geheime Schlüssel und das Berechtigungszertifikat auf einer externen Komponente, wie zum Beispiel einer Chipkarte, gespeichert sein. Hierzu kann die Computermaus **100** ein Chipkartenlesegerät beinhalten, welches zum Einführen einer solchen Chipkarte dient, so dass das RFID-Lesegerät **126** über dieses Chipkartenlesegerät auf die Chipkarte zugreifen kann. Insbesondere kann das RFID-Lesegerät **126** diesbezüglich entsprechend DE 10 2006 027 253 A1 ausgebildet sein, deren Offenbarungsgehalt durch Bezugnahme mit zum Offenbarungsgehalt der vorliegenden Patentanmeldung gemacht wird.

[0047] Die Computermaus **100** kann ferner ein Mausrad (sogenanntes „mause wheel") **140** aufwei-

sen, welches beispielsweise zwischen einer linken und einer rechten Maustaste angeordnet sein kann. Das Mausrad **140** dient in dem ersten Betriebsmodus in üblicher Art und Weise zur Eingabe eines Navigationskommandos oder einer Nutzerauswahl über die graphische Nutzeroberfläche des Computers **116**. In dem zweiten Betriebsmodus kann das Mausrad deaktiviert, das heißt funktionslos sein, oder es kann zur Eingabe von Daten oder Nutzerkommandos in das RFID-Lesegerät **126** ausgebildet sein.

[0048] Die Computermaus **100** kann ferner ein Display **142** und/oder eine Tastatur **144** aufweisen, welche beispielsweise hinter dem Mausrad **140** in einem Rückenbereich der Oberseite **104** der Computermaus **100** angeordnet sein können, wie in der Fig. 1 dargestellt.

[0049] Auf dem Display **102** kann zum Beispiel eine Eingabeaufforderung des RFID-Lesegeräts **126** an den Nutzer ausgegeben werden, so dass dieser eine geheime Kennung, wie zum Beispiel eine PIN über die Tastatur **144** eingibt. Alternativ oder zusätzlich zu der Tastatur **144** kann ein Biometriesensor, insbesondere ein Fingerabdrucksensor oder eine Kamera für einen Irisscan, in dem Gehäuse der Computermaus **100** integriert sein, um ein entsprechendes biometrisches Merkmal von dem Benutzer alternativ oder zusätzlich zu der Kennung zu erfassen. Die Kennung und/oder das biometrische Merkmal können zur Authentifizierung des Benutzers gegenüber dem Dokument **200**, zum Beispiel nach dem PACE-Protokoll dienen.

[0050] In dem zweiten Betriebsmodus kann beispielsweise so vorgegangen werden, dass zunächst der Nutzer seine PIN über die Tastatur **144** eingibt, um sich über das RFID-Lesegerät **126** gegenüber dem Dokument **200** zu authentifizieren. Ferner wird die Strahlungsquelle **120** eingeschaltet, so dass der optische Sensor **118** den Teilbereich des Dokuments einscannt und die darin beinhaltete Information erfasst, welche in das RFID-Lesegerät **126** eingegeben wird, um in dem zwischen dem RFID-Lesegerät **126** und dem Dokument **200** ablaufenden krytographischen Protokoll verwendet zu werden.

[0051] Beispielsweise wird durch Durchführung der Programminstruktionen **134** aus der Information ein kryptographischer Schlüssel abgeleitet, der Voraussetzung dafür ist, dass das RFID-Lesegerät **126** auf das Dokument **200** lesend zugreifen kann. Für eine solche Berechtigungsprüfung kann ferner der geheime Schlüssel benötigt werden, insbesondere zur Durchführung eines Challenge-Response-Protokolls, sowie das Berechtigungszertifikat, vergleiche hierzu auch die technische Richtlinie des BSI TR-03110.

[0052] Nachdem die Berechtigungsprüfung erfolgreich abgeschlossen worden ist und die Daten aus dem Dokument **200** gelesen worden sind, werden diese über die Schnittstelle **112** durch Signale **146** an die Schnittstelle **114** des Computers **116** übertragen.

[0053] Die Auswahl des ersten oder des zweiten Betriebsmodus kann durch ein Bedienelement der Computermaus erfolgen, beispielsweise über die Tastatur **144**. Ferner kann die Umschaltung des Betriebsmodus automatisch dann erfolgen, wenn zum Beispiel durch den optischen Sensor **118** oder den Bewegungssensor **106** sensiert wird, dass die Computermaus **100** von der Unterlage **108** abgehoben worden ist, da dies darauf hindeutet, dass der Benutzer das Dokument **200** unter die Computermaus **100** legen möchte oder das Dokument **200** von dort entfernen möchte. Ferner kann die Umschaltung des Betriebsmodus zum Beispiel durch Drücken des Mausrads **140** erfolgen. Eine weitere Möglichkeit ist, dass die Auswahl des Betriebsmodus mit Hilfe eines Anwendungsprogramms **148** erfolgt, welches von einem Prozessor **150** des Computers **116** ausgeführt wird und welches mit der Computermaus **100** interoperabel ist. Insbesondere kann das Anwendungsprogramm **148** ein Treiberprogramm für die Computermaus **100** beinhalten. Das Anwendungsprogramm **148** kann auch zumindest Teile des kryptographischen Protokolls implementieren, so dass der Prozessor **132** weniger leistungsfähig sein kann.

[0054] Die in Form der Signale **146** von der Computermaus **100** an den Computer **116** übertragenen Daten können dort lokal zum Beispiel von dem Anwendungsprogramm **148** weiter verarbeitet werden.

[0055] Alternativ oder zusätzlich hat der Computer **116** eine Netzwerkschnittstelle zu einem Netzwerk **152**, wie zum Beispiel dem Internet, haben, über welche der Computer **116** mit einem ID-Provider-Computersystem **154** und ein Dienst-Computersystem **156** verbunden ist. In diesem Fall werden die Daten über die Signale **146** mit Ende-zu-Ende-Verschlüsselung zwischen dem Dokument **200** und dem ID-Provider-Computersystem **154** übertragen. Die Daten können in diesem Fall Attribute beinhalten, welche von dem ID-Provider-Computersystem **154** signiert und an das Dienst-Computersystem **156** weitergeleitet werden, wie es an sich zum Beispiel aus DE 10 2008 000 067 A1 bekannt ist; in diesem Fall sind der geheime Schlüssel und das Berechtigungszertifikat dem ID-Provider-Computersystem **154** zugeordnet.

[0056] Die Prüfung des optischen Sicherheitsmerkmals wird lokal von der Computermaus **100**, zum Beispiel durch die Logik **124** oder durch Ausführung der Programminstruktionen **134** durchgeführt, und/oder das von dem optischen Sensor **118** aufgenommene Bild des oder der Sicherheitsmerkmale wird über die Schnittstelle **112** an den Computer **116** übertragen, welcher diese Auswertung vornimmt.

[0057] Die Fig. 2 zeigt ein Dokument **200** mit einem optischen Sicherheitsmerkmal **204**, wie zum Beispiel einem Passbild, dem Teilbereich **202** mit zum Beispiel der MRZ und/oder CAN sowie einem in den Dokumentenkörper des Dokuments **200** integrierten RFID-Chip **206**. Der RFID-Chip **206** hat eine RF-Schnittstelle **208**, die an eine in dem Dokumentenkörper des Dokuments **200** verlaufende Antennenspule angeschlossen ist und welche mit der RF-Schnittstelle **128** eine RF-Kommunikation ermöglicht.

[0058] Der RFID-Chip **206** hat ferner einen Speicher **210** mit einem geschützten Speicherbereich zur Speicherung eines Datenobjekts **212** sowie von Programminstruktionen **214** und Programminstruktionen **216** zur Ausführung durch einen Prozessor **218** des RFID-Chips **206**, durch welche zum Beispiel zwei verschiedene kryptographische Protokolle I bzw. II implementiert werden. Beispielsweise handelt es sich bei dem Protokoll I um das vom BSI spezifizierte PACE-Protokoll, das heißt ein Passwort-basiertes Diffie-Hellman-Schlüssel-Vereinbarungsprotokoll, wozu die Eingabe der Kennung, das heißt eines Passworts, zum Beispiel über die Tastatur **144** erforderlich ist.

[0059] Das Protokoll II kann dagegen sowohl ein BAC- als auch ein EAC-Protokoll implementieren, beispielsweise so wie von der ICAO spezifiziert. Das Dokument **200** unterstützt also die beiden alternativen Protokolle I und II, deren erfolgreiche Durchführung jeweils eine Voraussetzung für einen externen Lesezugriff auf das Datenobjekt **212** sind.

[0060] Die Programminstruktionen **134** implementieren die das RFID-Lesegerät **126** betreffenden Schritte zumindest eines dieser kryptographischen Protokolle I oder II. Wenn beispielsweise die Programminstruktionen **134** das Protokoll I unterstützen, so wird dieses zur Durchführung der Berechtigungsprüfung vor einem Lesezugriff durchgeführt, im gegenteiligen Fall das Protokoll II. Beispielsweise kann so vorgegangen werden, dass zunächst immer die Durchführung des Protokolls I versucht wird; wenn dieser Versuch fehlschlägt, wird anschließend die Durchführung des Protokolls II versucht.

[0061] Die Fig. 3 zeigt ein entsprechendes Flussdiagramm.

[0062] In dem Schritt **300** wird die Computermaus zunächst in ihrem ersten Betriebsmodus in üblicher Art und Weise zur Bewegung eines Cursors auf einer graphischen Nutzerschnittstelle (Graphical User Interface – GUI) verwendet. Zur Durchführung eines Lesezugriffs auf das Dokument **200** wird dann in dem Schritt **302** der zweite Betriebsmodus der Computermaus ausgewählt. Die Computermaus wird von dem Benutzer auf das Dokument gestellt oder geschoben, so dass sich das Dokument zwischen der Unterlage und der Unterseite der Computermaus befindet. In dem Schritt **304** erfolgt die Erfassung der Information aus dem Teilbereich des Dokuments durch den optischen Sensor **118** sowie optional auch die Erfassung optischer Sicherheitsmerkmale des Dokuments sowie deren Überprüfung.

[0063] Mit Hilfe der in dem Schritt **304** erfassten Information wird anschließend ein kryptographisches Protokoll zur Durchführung der Berechtigungsprüfung durchgeführt, beispielsweise das Protokoll I oder II. Hierzu kann es erforderlich sein, dass der Nutzer über die Tastatur **144** der Computermaus **100** oder über die Tastatur des Computers **116** eine Kennung eingibt und/oder dass von dem Benutzer ein biometrisches Merkmal erfasst wird. Ferner kann es für die Durchführung des kryptographischen Protokolls je nach Ausführungsform erforderlich sein, dass das RFID Lesegerät **126** auf einen Speicher zugreifen kann, in dem ein valides Berechtigungszertifikat gespeichert ist.

[0064] In der hier betrachteten Ausführungsform wird in dem Schritt **306** aus der erfassten Information, das heißt beispielsweise aus der MRZ oder der CAN, ein symmetrischer kryptographischer Schlüssel abgeleitet, der zur Verschlüsselung der nachfolgenden Kommunikation zwischen dem RFID-Lesegerät **126** und dem RFID-Chip **206** verwendet wird. Anschließend erfolgt eine Berechtigungsprüfung mit Hilfe des Berechtigungszertifikats zum Beispiel nach einem Challenge-Response-Protokoll in dem Schritt **310** für eine kryptographische Authentifizierung zum Beispiel des RFID-Lesegeräts **126**, nachdem zuvor in dem Schritt **308** auf das Berechtigungszertifikat zugegriffen worden ist.

[0065] In dem Schritt **312** wird dann geprüft, ob das kryptographische Protokoll erfolgreich durchgeführt und in dem Berechtigungszertifikat ausreichende Zugriffsrechte spezifiziert sind. ist dies nicht der Fall, wird in dem Schritt **314** abgebrochen. Im gegenteiligen Fall, wird in dem Schritt **316** mit Hilfe eines Lesekommandos auf das Datenobjekt **212** zugegriffen, was anschließend in dem Schritt **318** je nach Ausführungsform verschlüsselt oder unverschlüsselt an das RFID-Lesegerät **126** übertragen und dann in dem Schritt **320** durch Signale **146** gesendet wird.

[0066] Die Fig. 4 zeigt eine Ausführungsform einer Computermaus **100** mit einer linken Maustaste **158** und einer rechten Maustaste **160**, zwischen denen das Mausrad **140** angeordnet ist. Zum Beispiel auf der Maustante **158** kann ein Fingerabdrucksensor **162** angeordnet sein, um einen Fingerabdruck eines Benutzers zu erfassen. Ein weiterer Fingerabdrucksensor kann auf der anderen Maustaste **160** angeordnet sein, so dass gleichzeitig ein Fingerabdruck vom Zeigefinger und vom Mittelfinger eines Benutzers erfasst werden können.

[0067] Die Fig. 5 zeigt eine Ausführungsform einer Computermaus **100** mit einem Trackball **164**. In dem ersten Betriebsmodus der Computermaus **100** wird bei dieser Ausführungsform nicht die Relativbewegung der Computermaus **100** zu der Unterlage **108**, sondern die Bewegung des Trackballs **164** relativ zum Gehäuse der Computermaus **100** erfasst. Ansonsten ist die Funktionalität der Computermaus **100** analog zu den Ausführungsformen der Fig. 1 bis Fig. 4.

Bezugszeichenliste

100	Computermaus
102	Unterseite
104	Oberseite
106	Bewegungssensor
108	Unterlage
110	Signale
112	Schnittstelle
114	Schnittstelle
116	Computer
118	optischer Sensor
120	Strahlungsquelle
122	Strahlungsquelle
124	Logikkomponente
126	RFID-Lesegerät
128	RF-Schnittstelle
130	Antennenwicklung
132	Prozessor
134	Programminstruktionen
136	Speicherbereich
138	Speicherbereich
140	Mausrad
142	Display
144	Tastatur
146	Signale
148	Anwendungsprogramm
150	Prozessor
152	Netzwerk
154	ID-Providercomputersystem
156	Dienst-Computersystem
158	Maustaste
160	Maustaste
162	Fingerabdrucksensor
164	Trackball
200	Dokument
202	Teilbereich
204	Optisches Sicherheitsmerkmal
206	RFID-Chip
208	RF-Schnittstelle
210	Speicher
212	Datenobjekt
214	Speicherbereich
216	Speicherbereich
218	Prozessor

ZITATE ENTHALTEN IN DER BESCHREIBUNG

Diese Liste der vom Anmelder aufgeführten Dokumente wurde automatisiert erzeugt und ist ausschließlich zur besseren Information des Lesers aufgenommen. Die Liste ist nicht Bestandteil der deutschen Patent- bzw. Gebrauchsmusteranmeldung. Das DPMA übernimmt keinerlei Haftung für etwaige Fehler oder Auslassungen.

Zitierte Patentliteratur

- DE 19858935 A1 [**0002**]
- DE 10260924 B3 [**0002**]
- DE 102004023845 A1 [**0002**]
- EP 2254325 A1 [**0002**]
- EP 1891607 B1 [**0012**]
- DE 102006027253 A1 [**0046**]
- DE 102008000067 A1 [**0055**]

Zitierte Nicht-Patentliteratur

- Standard ISO14443 [**0007**]
- TR-03110 [**0012**]
- Standard X.509 [**0025**]
- TR-03110 [**0028**]
- Richtlinie des BSI TR-03110 [**0051**]

Patentansprüche

1. Computermaus mit zumindest einem ersten an der Unterseite (**102**) der Computermaus angeordneten optischen Sensor (**118**), der zum Einscannen zumindest eines Teilbereichs (**202**) eines Dokuments (**200**) ausgebildet ist, und mit einer RF-Schnittstelle (**128**) für eine drahtlose Kommunikation mit einem RFID-Chip (**206**) des Dokuments, wobei die Computermaus einen ersten Betriebsmodus zur Erfassung einer Position oder Bewegung der Computermaus relativ zu einer Unterlage und einem zweiten Betriebsmodus zur Durchführung eines Lesezugriffs auf den RFID-Chip des Dokuments aufweist, wobei die Computermaus für das Einscannen des Teilbereichs in dem zweiten Betriebsmodus zur Ermöglichung einer Berechtigungsprüfung für den Lesezugriff ausgebildet ist, und mit Prozessormitteln (**132**, **134**) zur Ausführung von Schritten eines kryptographischen Protokolls für die Durchführung der Berechtigungsprüfung.

2. Computermaus nach Anspruch 1, mit einer Infrarotstrahlungsquelle (**120**), wobei der erste optische Sensor in einem Infrarotspektralbereich strahlungssensitiv ist.

3. Computermaus nach Anspruch 2, mit einer Strahlungsquelle (**122**), die zur Abgabe von Licht in einem sichtbaren Spektralbereich ausgebildet ist, insbesondere mit einer Weißlichtstrahlungsquelle, wobei der erste optische Sensor zusätzlich im Bereich des von der Strahlungsquelle abgegebenen sichtbaren Spektralbereichs strahlungssensitiv ist, um eine Erfassung eines optischen Sicherheitsmerkmals des Dokuments zu ermöglichen.

4. Computermaus nach Anspruch 1, 2 oder 3, wobei der erste optische Sensor als eine Kamera mit einem Objektiv ausgebildet ist.

5. Computermaus nach einem der vorhergehenden Ansprüche, wobei der erste optische Sensor in dem ersten Betriebsmodus als Bewegungssensor wirkt.

6. Computermaus nach einem der vorhergehenden Ansprüche 1 bis 4, mit einem zweiten Sensor (**106**), der in dem ersten Betriebsmodus als Positions- oder Bewegungssensor dient.

7. Computermaus nach einem der vorhergehenden Ansprüche, mit einer an die RF-Schnittstelle angeschlossene Antenne, wobei die Antenne ein oder mehrere Antennenwicklungen (**130**) aufweist, deren Öffnung auf die Unterseite der Computermaus ausgerichtet ist.

8. Computermaus nach einem der vorhergehenden Ansprüche, mit Eingabemitteln (**144**) zur Eingabe einer Kennung, insbesondere einer PIN, wobei die Prozessormittel dazu ausgebildet sind, die eingegebene Kennung für die Ausführung des kryptographischen Protokolls zu verwenden.

9. Computermaus nach einem der vorhergehenden Ansprüche, mit einer Anzeigevorrichtung (**142**), welche vorzugsweise an der Oberseite (**104**) der Computermaus, insbesondere deren Rückenbereich, angeordnet ist.

10. Computermaus nach einem der vorhergehenden Ansprüche mit einem Biometriesensor (**162**), insbesondere einem Fingerabdrucksensor, zur Erfassung eines biometrischen Merkmals eines Benutzers, wobei das erfasste biometrische Merkmal in den kryptographischen Algorithmus eingeht.

11. Computermaus nach einem der vorhergehenden Ansprüche mit einem Bedienelement (**158**, **160**) zur Wahl des ersten oder des zweiten Betriebsmodus.

12. Computermaus nach einem der vorhergehenden Ansprüche, mit Zugriffsmitteln (**132**, **134**) zum Zugriff auf ein Berechtigungszertifikat, um gegenüber dem RFID-Chip des Dokuments die Berechtigung für den Lesezugriff auf die Daten nachzuweisen.

13. Computermaus nach Anspruch 12, mit einem Speicher (**138**) zur Speicherung des Berechtigungszertifikats, wobei die Zugriffsmittel zur Zugriff auf den Speicher ausgebildet sind, um das Berechtigungszertifikat auszulesen.

14. Elektronisches System mit zumindest einem Computer (**116**, **154**, **156**) und einer Computermaus (**100**) nach einem der vorhergehenden Ansprüche 1 bis 13, wobei der Computer dazu ausgebildet ist, in dem ersten Betriebsmodus der Computermaus erste Signale (**110**) von der Computermaus zu empfangen, die die Bewegung oder die Position der Computermaus auf einer Unterlage (**108**) anzeigen, und wobei der Computer dazu ausgebildet ist, in dem zweiten Betriebsmodus zweite Signale (**146**) von der Computermaus zu empfangen, welche aus dem RFID-Chip (**206**) des Dokuments ausgelesene Daten (**212**) beinhalten.

15. Elektronisches System nach Anspruch 14, wobei auf dem Computer ein Anwendungsprogramm (**148**) zur Kommunikation mit der Computermaus und zur Wahl des ersten oder zweiten Betriebsmodus installiert ist.

16. Verfahren zum Lesen von Daten aus einem Dokument mit Hilfe eines elektronischen Systems nach Anspruch 14 oder 15, wobei das Dokument eine optisch lesbare Information und einen RFID-Chip aufweist, in dem geschützte Daten gespeichert sind, mit folgenden Schritten:

– Auswahl des zweiten Betriebsmodus der Computermaus,
– Lesen der Information von dem Dokument durch den ersten optischen Sensor,
– Durchführung eines kryptographischen Protokolls mit dem RFID-Chip, wobei die Information in den kryptographischen Algorithmus eingeht,
– Durchführung eines Lesezugriffs auf die Daten unter der Voraussetzung, dass der kryptographische Algorithmus erfolgreich durchgeführt worden ist,
– Übertragung der Daten von der Computermaus an den Computer.

17. Verfahren nach Anspruch 16, wobei sich die Computermaus initial in ihrem ersten Betriebsmodus befindet, und durch eine Benutzereingabe in das Anwendungsprogramm des Computers der zweite Betriebsmodus ausgewählt wird.

18. Verfahren nach Anspruch 17, wobei die Auswahl des zweiten Betriebsmodus mit Hilfe der Computermaus erfolgt.

Es folgen 4 Blatt Zeichnungen

Anhängende Zeichnungen

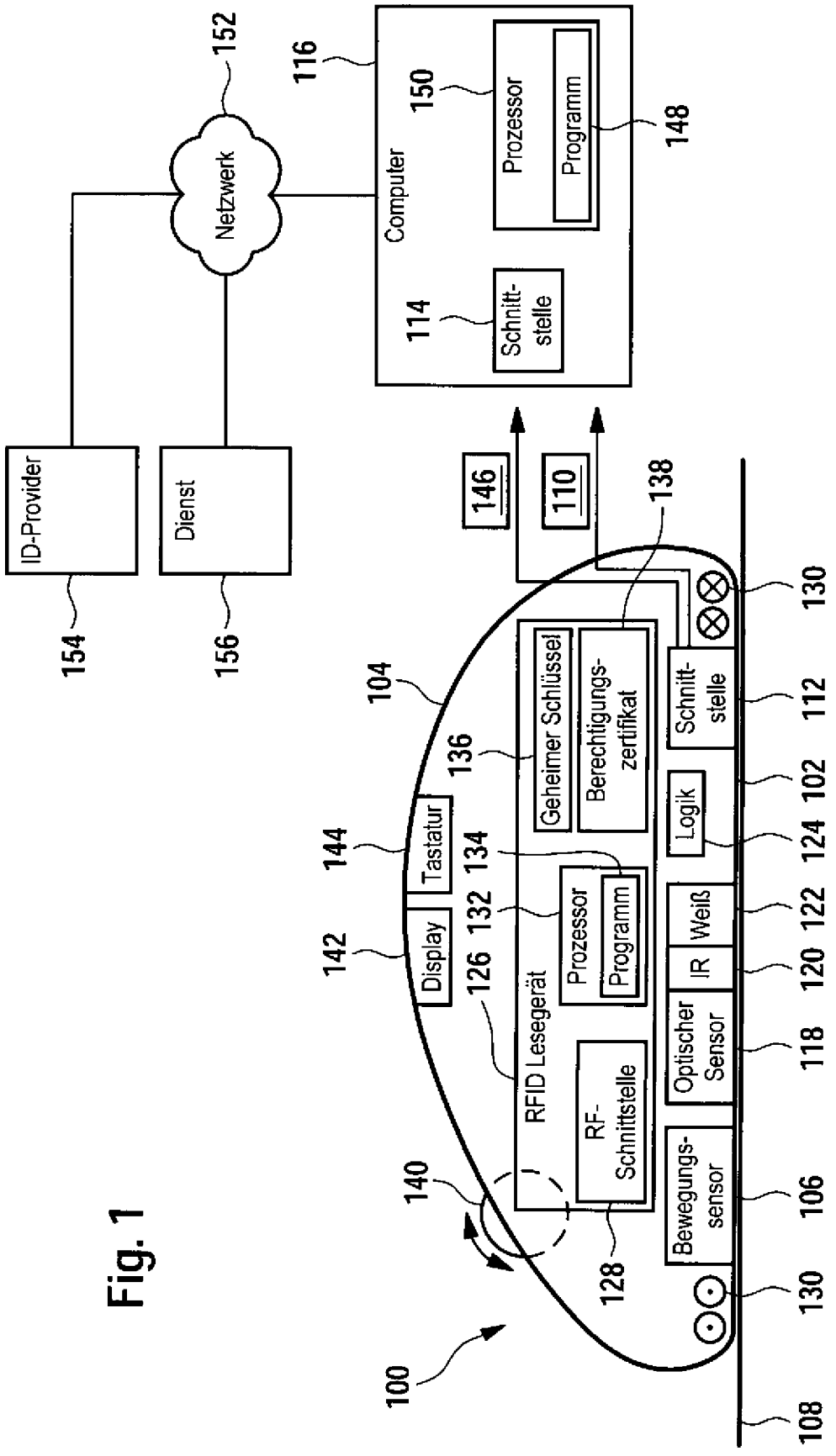


Fig. 1

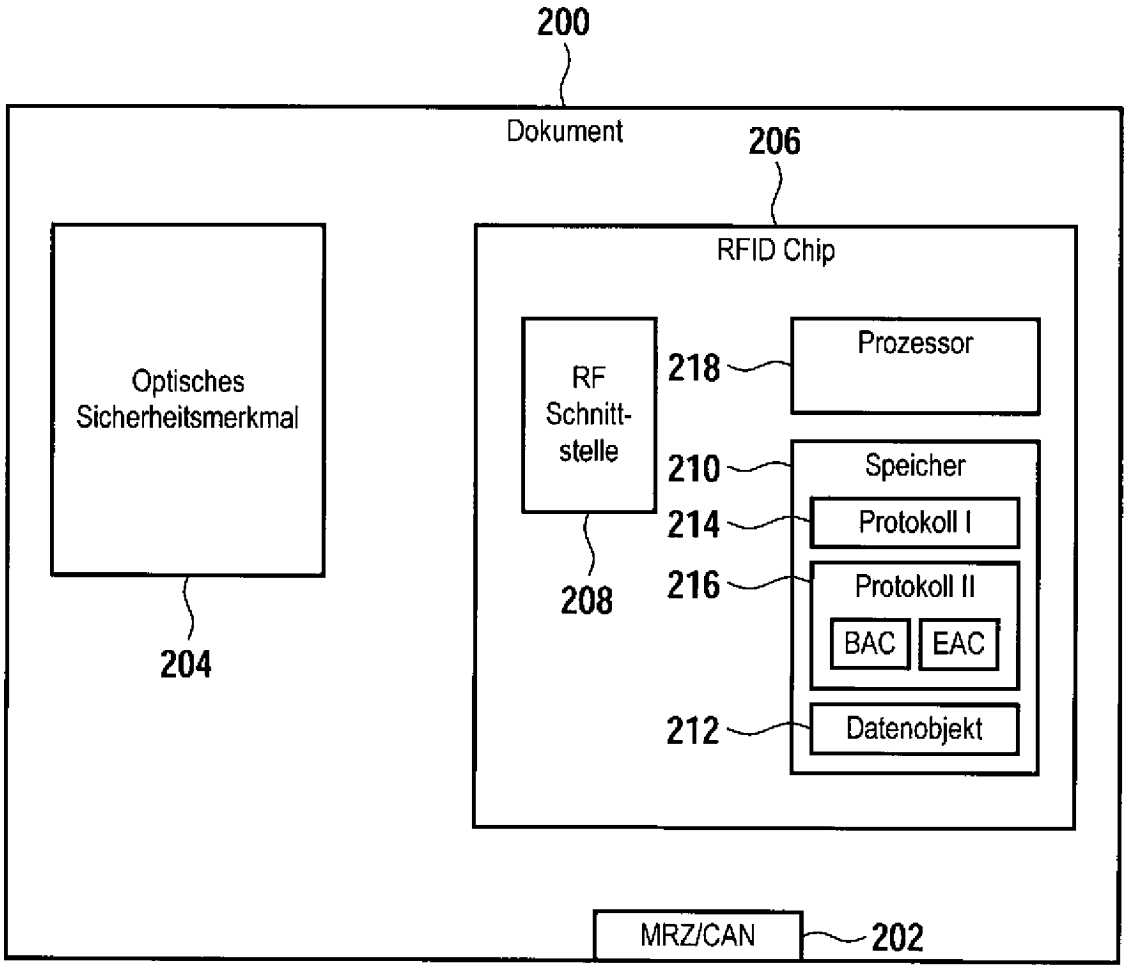

200
Dokument
206
RFID Chip
Optisches Sicherheitsmerkmal
204
RF Schnitt-stelle
208
218
Prozessor
210
Speicher
214
Protokoll I
216
Protokoll II
BAC
EAC
212
Datenobjekt
MRZ/CAN
202

Fig. 2

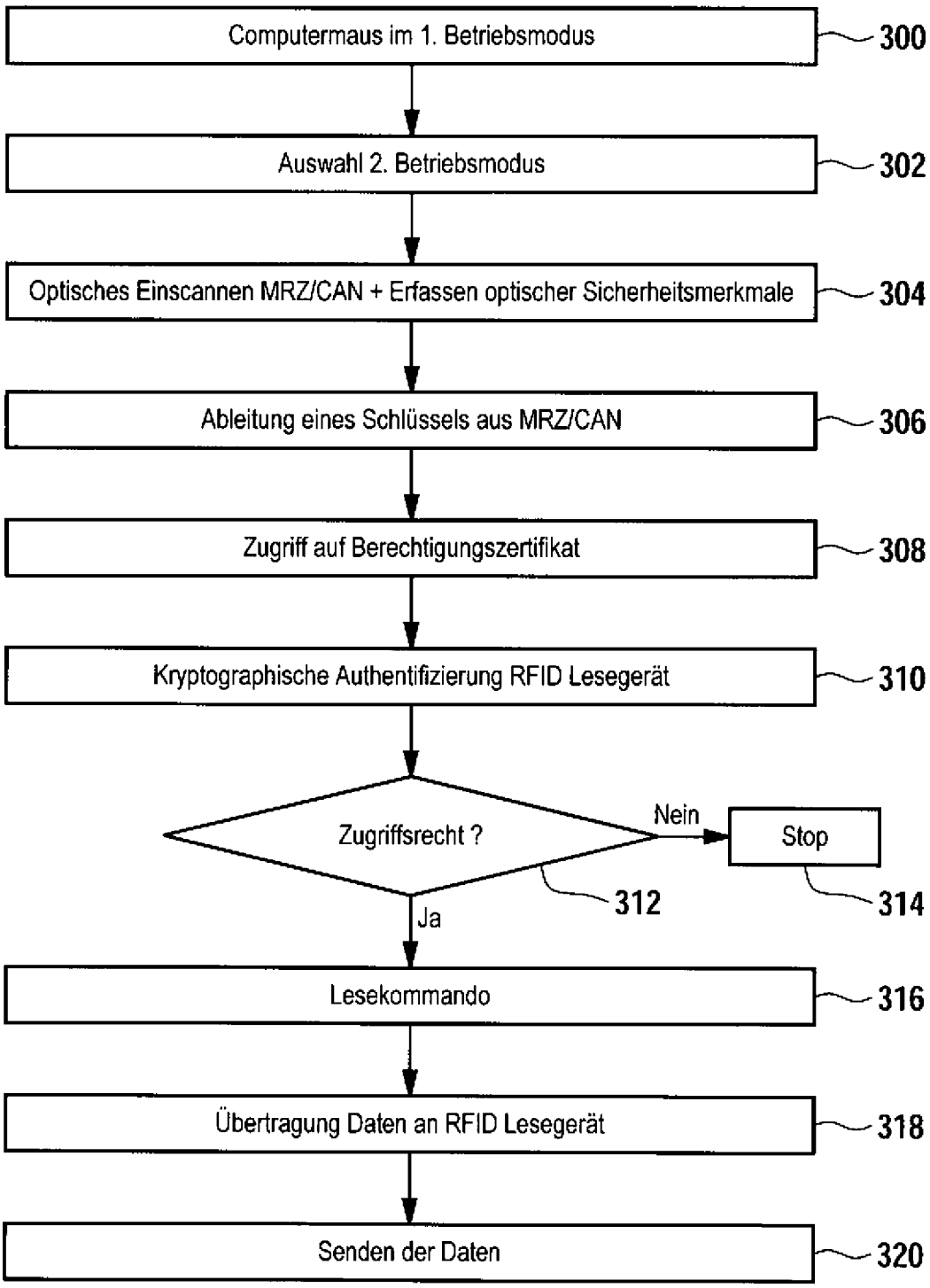

Computermaus im 1. Betriebsmodus
300
Auswahl 2. Betriebsmodus
302
Optisches Einscannen MRZ/CAN + Erfassen optischer Sicherheitsmerkmale
304
Ableitung eines Schlüssels aus MRZ/CAN
306
Zugriff auf Berechtigungszertifikat
308
Kryptographische Authentifizierung RFID Lesegerät
310
Zugriffsrecht ?
Nein
Stop
312
314
Ja
Lesekommando
316
Übertragung Daten an RFID Lesegerät
318
Senden der Daten
320

Fig. 3

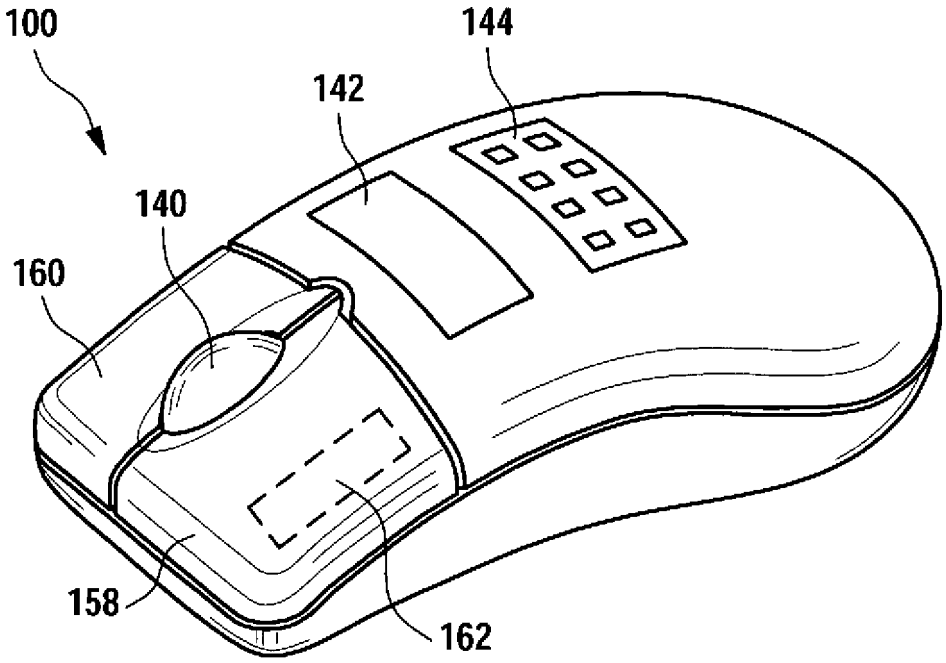


Fig. 4

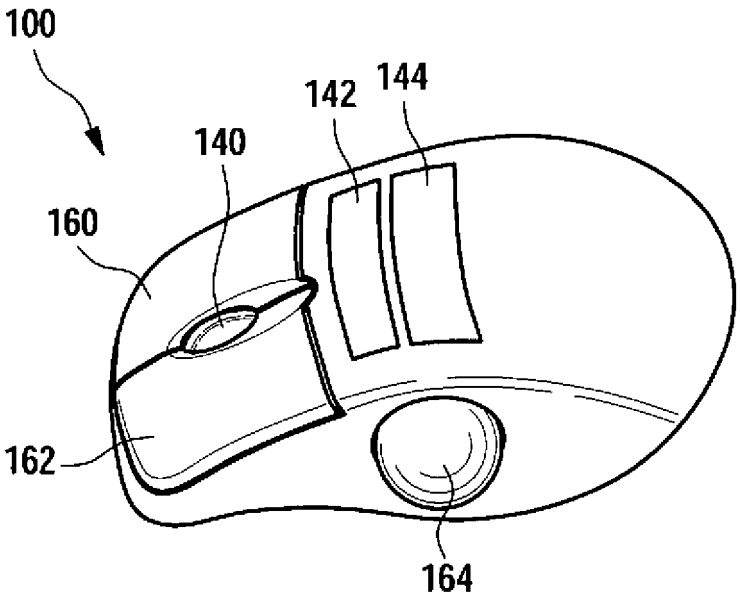


Fig. 5