(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 10 2007 000 589 B9** 2010.01.28

(12) # Berichtigung der Patentschrift

(21) Aktenzeichen: **10 2007 000 589.1**
(22) Anmeldetag: **29.10.2007**
(43) Offenlegungstag: **–**
(45) Veröffentlichungstag der Patenterteilung: **09.07.2009**
(15) Korrekturinformation:
Berichtigung in Anspruch 1
(48) Veröffentlichungstag der Berichtigung: **28.01.2010**

(51) Int Cl.[8]: ***H04L 9/32*** (2006.01)
H04L 9/12 (2006.01)
H04L 9/28 (2006.01)
G06K 19/073 (2006.01)

(73) Patentinhaber:
Bundesdruckerei GmbH, 10969 Berlin, DE

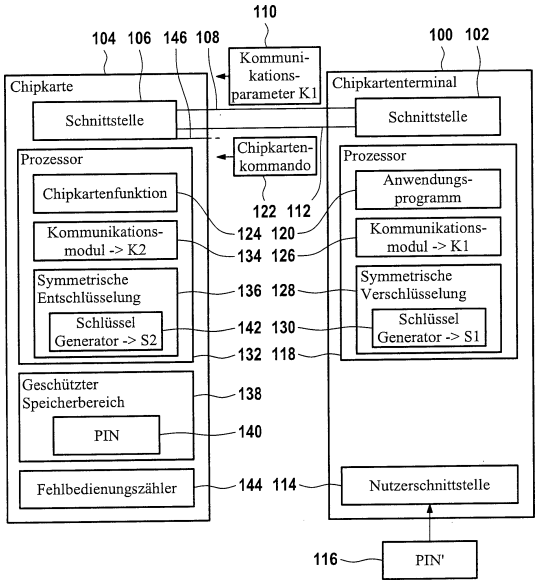
(74) Vertreter:
Richardt, M., Dipl.-Ing., Pat.-Anw., 65343 Eltville

(72) Erfinder:
Nguyen, Kim, Dr., 10437 Berlin, DE; Byszio, Frank, 16348 Wandlitz, DE

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

(54) Bezeichnung: **Verfahren zum Schutz einer Chipkarte gegen unberechtigte Benutzung, Chipkarte und Chipkarten-Terminal**

(57) Hauptanspruch: Verfahren zum Schutz einer Chipkarte (104) gegen unberechtigte Benutzung mit folgenden Schritten:
– Eingabe einer ersten Kennung (116) in einen Chipkarten-Terminal (100),
– Erzeugung eines Chiffrats aus zumindest einem ersten Kommunikationsparameter (K1; KA1, D1) mit Hilfe eines aus der ersten Kennung abgeleiteten ersten symmetrischen Schlüssels (S1), wobei mit Hilfe des Kommunikationsparameters ein geschützter erster Kommunikationskanal (112) zwischen dem Chipkarten-Terminal und der Chipkarte definierbar ist,
– Übertragung des Chiffrats über einen vordefinierten Kommunikationskanal (108) von dem Chipkarten-Terminal an die Chipkarte,
– Versuch einer Entschlüsselung des Chiffrats mit Hilfe eines zweiten symmetrischen Schlüssels (S2) durch die Chipkarte, wobei das Resultat der Entschlüsselung nur dann der erste Kommunikationsparameter ist, wenn der erste symmetrische Schlüssel dem zweiten symmetrischen Schlüssel gleicht, sodass der geschützte erste Kommunikationskanal nur dann zwischen dem Chipkarten-Terminal und der Chipkarte definierbar ist, wenn die erste Kennung zutreffend ist.



Die oben angegebenen bibliographischen Daten entsprechen dem aktuellen Stand zum Zeitpunkt der Veröffentlichung dieser Berichtigung.

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

(10) **DE 10 2007 000 589 B9**

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

DE	**198 50 307**	**C2**
DE	**195 07 044**	**C2**
DE	**195 07 043**	**A1**
DE	**35 23 237**	**A1**
US	**71 39 917**	**B2**
US	**67 92 533**	**B2**
US	**2005/01 82 934**	**A1**
US	**2003/00 14 370**	**A1**
US	**52 41 599**	**A**
EP	**07 30 253**	**B1**
EP	**10 22 638**	**A2**

Jablon,D.: Strong Password-Only Authenticated Key Exchange. 02. März 1997, Im Internet: <URL:http:www.jablon.org/speke97.html>

Borchers,D.: PACE für die schnelle Authentifizierung. Heise Online, 08.02.2007. Im Internet: <URL:http.www.heise.de/securitynews/meldung/85024>

Barker,E., u.a.: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography. National Institute of Standards and Technology (NIST), NIST Special Publication 800- 56A, März 2007. Im Internet: <URL:http://csrc.nist.gov/publications/nistpubs/800-56A/SP800-56A_Revision1_Mar08-2007.pdf>

SEC1: Elliptic Curve Cryptography. Standards for Efficient Cryptography, Certicom Research, 20. September 2000, Version 1.0. Im Internet: <URL:http://www.secg.org/download/aid-385/sec1_final.pdf>

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zum Schutz einer Chipkarte gegen unberechtigte Benutzung, eine Chipkarte und ein Chipkarten-Terminal.

[0002] Für die Freischaltung einer Chipkarten-Funktion kann eine zuvorige Benutzeridentifizierung gegenüber der Chipkarte erforderlich sein, wie es aus dem Stand der Technik an sich bekannt ist. Die häufigste Benutzeridentifizierung ist die Eingabe einer geheimen Kennung, welche im Allgemeinen als PIN (Personal Identification Number) oder als CHV (Card Holder Verification) bezeichnet wird. Solche Kennungen bestehen im Allgemeinen aus einer numerischen oder alphanumerischen Zeichenkette. Zur Benutzeridentifizierung wird die Kennung von dem Benutzer auf der Tastatur eines Chipkarten-Terminals oder eines Computers, an den ein Chipkarten-Leser angeschlossen ist, eingegeben, und dann zu der Chipkarte gesendet. Diese vergleicht die eingegebene Kennung mit der gespeicherten Kennung und teilt dann das Ergebnis dem Terminal bzw. dem Computer durch Ausgabe eines entsprechenden Signals mit.

[0003] Bei den PINs kann zwischen statischen und änderbaren Pins unterschieden werden. Eine statische PIN ist vom Benutzer nicht mehr veränderbar und muss von diesem auswendig gelernt werden. Ist sie bekannt geworden, dann muss der Kartenbenutzer seine Chipkarte zerstören, um Missbrauch durch Unbefugte zu unterbinden, und sich eine neue Chipkarte mit einer anderen statischen PIN besorgen. Ebenso braucht der Benutzer eine neue Chipkarte, wenn er oder sie die statische PIN vergessen hat.

[0004] Eine änderbare PIN kann vom Benutzer nach Belieben geändert werden. Zum Ändern der PIN ist es aus Sicherheitsgründen immer notwendig, die aktuell gültige PIN mit zu übergeben, da sonst jede bestehende PIN durch einen Angreifer mit seiner eigenen ersetzt werden könnte.

[0005] Anders verhält es sich mit den so genannten Super-PINs oder PUKs (Personal Unlocking Key). Diese haben in der Regel mehr Stellen als die eigentliche PIN, und werden dazu benutzt, einen auf seinem Maximalwert stehenden Fehleingabezähler (wird auch als ”Fehlbedienungszähler” bezeichnet) einer PIN wieder zurückzusetzen. Mit der PUK wird auch gleich eine neue PIN an die Chipkarte übergeben, weil ein zurückgesetzter Fehlbedienungszähler wenig nützt, wenn man die PIN vergessen hat. Und dies ist ja meist der Fall, wenn der Fehlbedienungszähler seinen Maximalwert erreicht hat.

[0006] Es gibt auch Anwendungen, die Transport-PINs verwenden. Die Chipkarte wird mit einer zufälligen PIN personalisiert, welche der Kartenbenutzer in einem PIN-Brief erhält. Bei der ersten Eingabe wird er aber von der Chipkarte dazu aufgefordert, die personalisierte PIN durch seine eigene zu ersetzen. Bei einem ähnlichen Verfahren, „Null-PIN-Verfahren” genannt, wird die Chipkarte mit einer Trivial-PIN, wie etwa „0000” vorbelegt, und es wird ebenfalls von der Chipkarte bei der ersten Benutzung ein Wechsel erzwungen (vgl. hierzu auch DE 35 23 237 A1, DE 195 07 043 A1, DE 195 07 044 C2, DE 198 50 307 C2, EP 0 730 253 B1). Durch solche Verfahren ist eine sog. Erstbenutzerfunktion gegeben, die dem autorisierten Benutzer Sicherheit darüber verschafft, dass vor dessen Erbenutzung keine unerlaubte Nutzung der Chipkarte durch einen Dritten stattgefunden hat.

[0007] Aus der DE 198 50 307 C2 ist ein Verfahren zum Schutz vor Missbrauch bei Chipkarten bekannt. Die Chipkarte hat eine Erstnutzerfunktion, die bei der erstmaligen Benutzung der Daten und/oder Funktionen der Chipkarte die Vorgabe einer vom Benutzer beliebig wählbaren, persönlichen Geheimzahl (PIN) fordert, wobei durch die Eingabe der persönlichen Geheimzahl Daten und/oder Funktionen der Chipkarte in einen Benutzt-Status gesetzt werden. Eine spätere Änderung der persönlichen Geheimzahl wird durch einen übergeordneten Entsperrcode ermöglicht.

[0008] Aus dem Stand der Technik sind auch bereits Verfahren zur Überprüfung einer Kennung bekannt geworden, bei denen die Übertragung der Kennung selbst nicht erforderlich ist, wie zum Beispiel Strong Password Only Authentication Key Exchange (SPEKE), Diffie-Hellman Encripted Key Exchange (DH-EKE), Bellovin-Merritt Protokoll oder Password Authenticated Connection Establishment (PACE). Das SPEKE-Protokoll ist beispielsweise bekannt aus www.jablon.org/speke97.html, US 6,792,533 B2 und US 7,139,917 B2. Unter anderem ebenfalls aus www.jablon.org/speke97.html ist das DH-EKE-Protokoll bekannt. Unter anderem aus US 5,241,599 ist das Bellovin-Merritt-Protokoll bekannt. Aus www.heise.de/security/news/meldung/85024 ist das PACE-Protokoll bekannt, welches sich besonderes für elliptische Kurven-Kryptographie eignet.

[0009] Die Druckschrift US 2003/0014370 A1 beschreibt ein Kartenlesegerät, welches mit einem Rechnungsakzeptor kombiniert ist. Das Kartenlesegerät und eine Chipkarte können sich über ein in diesem Dokument beschriebenes Verfahren gegenseitig authentifizieren. Dazu erzeugt das Kartenlesegerät eine erste Zufallszahl, die vom Kartenlesegerät unter Verwendung eines gemeinsamen Schlüssels verschlüsselt wird, sodass eine verschlüsselte erste Zufallszahl generiert wird. Die Chipkarte generiert eine zweite Zufallszahl, die mittels desselben Schlüssels verschlüsselt wird, sodass eine verschlüsselte zweite Zufallszahl generiert wird. Die verschlüsselten Zufallszahlen werden zwischen dem Chipkartenlesege-

rät und der Chipkarte ausgetauscht. Das Lesegerät entschlüsselt die verschlüsselte zweite Zufallszahl unter Verwendung des gemeinsamen Schlüssels, wodurch das Lesegerät die zweite Zufallszahl erhält. Das Lesegerät generiert Sitzungsschlüssel mittels der ersten und der zweiten Zufallszahl. In ähnlicher Weise generiert die Chipkarte denselben Sitzungsschlüssel unter Verwendung der zweiten Zufallszahl und nach Entschlüsselung der verschlüsselten ersten Zufallszahl unter Verwendung des gemeinsamen Schlüssels. Die vom Lesegerät durch Entschlüsselung mit dem gemeinsamen Schlüssel ermittelte zweite Zufallszahl wird sodann mit dem Sitzungsschlüssel verschlüsselt und an die Chipkarte übermittelt. Ferner verschlüsselt die Chipkarte die erste Zufallszahl, die die Chipkarte zuvor durch Entschlüsselung der verschlüsselten ersten Zufallszahl mit dem gemeinsamen Schlüssel bestimmt hat, mittels des Sitzungsschlüssels. Das Ergebnis der Verschlüsselung wird an das Lesegerät übermittelt. Durch Entschlüsselung des Übermittelten kann nun die Chipkarte einerseits feststellen, ob das entschlüsselte Ergebnis der zweiten Zufallszahl entspricht, die ja zuvor von der Chipkarte generiert wurde. Andererseits kann das Lesegerät aus dem von der Chipkarte Übermittelten bestimmen, ob die mit dem Sitzungsschlüssel verschlüsselte erste Zufallszahl tatsächlich der Zufallszahl entspricht, die zu Beginn des Verfahrens vom Lesegerät generiert wurde. Falls das Lesegerät einerseits ermittelt, dass die verschlüsselt von der Karte empfangene erste Zufallszahl tatsächlich der ursprünglich vom Lesegerät generierten ersten Zufallszahl entspricht, und falls andererseits die Chipkarte feststellt, dass die verschlüsselt vom Lesegerät empfangene zweite Zufallszahl der ursprünglichen zweiten Zufallszahl, die von der Chipkarte generiert wurde, entspricht, ist die gegenseitige Authentifizierung zwischen Lesegerät und Chipkarte erfolgreich.

[0010] Die Druckschrift US 2005/0182934 A1 betrifft ein Verfahren und eine Vorrichtung zur Bereitstellung einer sicheren Kommunikation zwischen einem Computer und einer Karte, die einen Chip beinhaltet. Die Karte wird über eine USB-Schnittstelle an den Computer angeschlossen. Zur Initialisierung der Kommunikation mit der Karte wird ein Schlüssel zwischen der Karte und dem Computer generiert, indem der Computer einen öffentlichen Schlüssel von der Karte empfängt, einen zufälligen Schlüssel mit dem öffentlichen Kartenschlüssel verschlüsselt und diesen dann an die Karte übermittelt, woraus dann die Karte den zufälligen Schlüssel ermitteln kann, der dann als Schlüssel für die weitere Kommunikation dient.

[0011] Die Druckschrift EP 1022638 A2 beschreibt ein Verfahren und ein System zum sicheren Austausch von Informationen zwischen zwei Informationsverarbeitungsanlagen. Ein Informationsverarbeitungsgerät verschlüsselt seinen Schlüssel und weitere Informationen mit dem Schlüssel eines anderen Geräts und übermittelt die verschlüsselten Daten an dieses Gerät. Dieses Informationsverarbeitungsgerät entschlüsselt nun mit dem ihm bekannten Schlüssel die empfangenen Daten und erhält so den Schlüssel des sendenden Informationsverarbeitungsgeräts mit dem dann das Gerät die damit verschlüsselten Informationen entschlüsseln kann.

[0012] Demgegenüber liegt der Erfindung die Aufgabe zugrunde, ein verbessertes Verfahren zum Schutz einer Chipkarte gegen unberechtigte Benutzung zu schaffen. Der Erfindung liegt ferner die Aufgabe zugrunde, eine verbesserte Chipkarte und ein verbessertes Chipkarten-Terminal zu schaffen.

[0013] Die der Erfindung zugrunde liegenden Aufgaben werden jeweils mit den Merkmalen der unabhängigen Patentansprüche gelöst. Bevorzugte Ausführungsformen sind in den abhängigen Patentansprüchen angegeben.

[0014] Erfindungsgemäß wird ein Verfahren zum Schutz einer Chipkarte gegen unberechtigte Benutzung geschaffen. Das Verfahren involviert neben der Chipkarte selbst ein Chipkarten-Terminal.

[0015] Unter „Chipkarten-Terminal" wird hier jedes Gerät verstanden, welches zur Kommunikation mit einer Chipkarte ausgebildet ist, um beispielsweise Chipkarten-Kommandos an die Chipkarte zu richten und entsprechende Antworten von der Chipkarte zu empfangen. Die Kommunikation zwischen Chipkarte und Chipkarten-Terminal kann dabei kontaktbehaftet, drahtlos, beispielsweise über ein RFID-Verfahren, oder wahlweise kontaktbehaftet oder drahtlos erfolgen, insbesondere über eine so genannte Dual-Mode-Schnittstelle. Bei dem Chipkarten-Terminal kann es sich um ein so genanntes Klasse 1, 2 oder 3 Chipkarten-Lesegerät mit oder ohne eigener Tastatur oder einen Computer handeln, an den ein Chipkarten-Lesegerät angeschlossen ist. Bei dem Chipkarten-Terminal kann es sich auch um ein für einen bestimmten Zweck vorgesehenes Terminal handeln, wie zum Beispiel einen Bankterminal zur Abwicklung von Bankgeschäften, einen Bezahlterminal, beispielsweise zum Kauf elektronischer Tickets, oder einen Zugangsterminal zur Freigabe des Zugangs zu einem geschützten Bereich.

[0016] Unter dem Terminus „Schutz einer Chipkarte" wird hier der Schutz der Chipkarte insgesamt oder der Schutz von einer oder mehreren Chipkartenfunktionen der Chipkarte verstanden. Beispielsweise wird erfindungsgemäß eine besonders schützenswerte Chipkartenfunktion der Chipkarte geschützt, wie zum Beispiel eine Signaturfunktion zur Generierung einer elektronischen Signatur, eine Bezahlfunktion, eine Authentisierungsfunktion oder dergleichen.

[0017] Nach einer Ausführungsform des erfindungsgemäßen Verfahrens erhält der autorisierte Benutzer von der die Chipkarte ausgebenden Stelle eine geheime Kennung, die im Allgemeinen als PIN bezeichnet wird. Zur Benutzung der Chipkarte muss zunächst eine Kennung in den Chipkarten-Terminal eingegeben werden, die im Weiteren als PIN' bezeichnet wird. Nur wenn die PIN' identisch mit der PIN ist, soll eine Nutzung der Chipkarte bzw. der geschützten Chipkartenfunktion möglich sein.

[0018] Hierzu erzeugt der Chipkarten-Terminal ein Chiffrat aus zumindest einem ersten Kommunikationsparameter mit Hilfe eines ersten symmetrischen Schlüssels. Bei dem ersten symmetrischen Schlüssel kann es sich um die PIN' selbst handeln oder um einen von der PIN' abgeleiteten symmetrischen Schlüssel. Beispielsweise dient die PIN' als so genannter Seed Value zur Generierung des ersten symmetrischen Schlüssels durch das Chipkarten-Terminal.

[0019] Der zumindest eine Kommunikationsparameter ist so beschaffen, dass durch ihn ein geschützter ersten Kommunikationskanal zwischen dem Chipkarten-Terminal und der Chipkarte definierbar ist. Um diesen geschützten ersten Kommunikationskanal zwischen der Chipkarte und dem Chipkarten-Terminal aufbauen zu können, wird zunächst das mit Hilfe des ersten symmetrischen Schlüssels gewonnene Chiffrat des ersten Kommunikationsparameters über einen vordefinierten Kommunikationskanal von dem Chipkarten-Terminal an die Chipkarte übertragen. Dieser vordefinierte Kommunikationskanal ist also standardmäßig zum Aufbau einer initialen Kommunikation zwischen dem Chipkarten-Terminal und der Chipkarte definiert.

[0020] Nach der Übertragung des Chiffrats über diesen vordefinierten Kommunikationskanal von dem Chipkarten-Terminal an die Chipkarte wird seitens der Chipkarte der Versuch einer Entschlüsselung dieses Chiffrats mit Hilfe eines zweiten symmetrischen Schlüssels unternommen. Diese Entschlüsselung gelingt nur dann, wenn der zweite symmetrische Schlüssel gleich dem ersten Schlüssel ist, d. h. wenn die Voraussetzung PIN' = PIN erfüllt ist.

[0021] Der Aufbau einer Kommunikationsverbindung über den geschützten ersten Kommunikationskanal ist also nur dann möglich, wenn die Bedingung PIN' = PIN erfüllt ist, da die Chipkarte nur in diesem Fall Kenntnis von dem ersten Kommunikationsparameter erlangt, durch den der geschützte erste Kommunikationskanal festlegbar ist.

[0022] Bei dem ersten Kommunikationsparameter kann es sich beispielsweise um die Angabe einer Übertragungsfrequenz, eines Frequenz-Hopping-Schemas, eines Codierungs-Verfahrens und/oder eines Modulationsverfahrens handeln.

[0023] Wenn die Bedingung PIN' = PIN dagegen nicht erfüllt ist, so stimmt der aus der PIN' abgeleitete erste Schlüssel nicht mit dem zweiten Schlüssel der Chipkarte überein. Dies hat zur Folge, dass die Entschlüsselung des von dem Chipkarten-Terminal empfangenen Chiffrats durch die Chipkarte mit Hilfe des zweiten Schlüssels nicht den ersten Kommunikationsparameter hervorbringt, sondern beispielsweise einen zweiten Kommunikationsparameter, der von dem ersten Kommunikationsparameter abweicht.

[0024] Durch den zweiten Kommunikationsparameter kann ein zweiter Kommunikationskanal definiert sein, der von dem ersten Kommunikationskanal abweichend ist. Wenn die Chipkarte auf dem ersten Kommunikationskanal ein Signal empfängt, so wird dieses jedoch ignoriert, da die Chipkarte ein Signal auf dem zweiten Kommunikationskanal erwartet. Im Ergebnis kommt also keine Kommunikation zwischen dem Chipkarten-Terminal und der Chipkarte zustande, wenn die Bedingung PIN' = PIN nicht erfüllt ist.

[0025] Nach einer Ausführungsform der Erfindung kann es sich bei dem Kommunikationsparameter um einen öffentlichen Schlüssel eines asymmetrischen Schlüsselpaars des Chipkarten-Terminals handeln. Für die Festlegung eines symmetrischen Schlüssels für die Kommunikation zwischen dem Chipkarten-Terminal und der Chipkarte, beispielsweise nach dem Diffie-Hellman-Verfahren, wird der öffentliche Schlüssel des Chipkarten-Terminals mit dem aus der ersten Kennung gewonnenen ersten symmetrischen Schlüssel verschlüsselt und über den vordefinierten Kommunikationskanal an die Chipkarte gesendet.

[0026] Nur wenn die Bedingung PIN' = PIN erfüllt ist, erhält die Chipkarte den korrekten öffentlichen Schlüssel des Chipkarten-Terminals. Das Chipkarten-Terminal generiert aus dem öffentlichen Schlüssel der Chipkarte, der beispielsweise von einem Schlüssel-Server abgefragt wird, nach dem Diffie-Hellman-Verfahren den dritten Schlüssel, wohingegen die Chipkarte aus deren privaten Schlüssel und dem mit Hilfe des zweiten symmetrischen Schlüssels entschlüsselten Chiffrat einen vierten Schlüssel ebenfalls nach dem Diffie-Hellman-Verfahren generiert, wobei der vierte Schlüssel nur dann gleich dem dritten Schlüssel ist, wenn die Bedingung PIN' = PIN erfüllt ist.

[0027] Der dritte und der identische vierte symmetrische Schlüssel dient zur Verschlüsselung von Signalen, insbesondere Chipkarten-Kommandos und Antworten auf solche Chipkarten-Kommandos, die zwischen dem Chipkarten-Terminal und der Chipkarte über den ersten Kommunikationskanal ausgetauscht werden. Dieser erste Kommunikationskanal ist zumindest zusätzlich über den dritten Schlüssel

definiert, mit Hilfe dessen die Kommunikation über den ersten Kommunikationskanal mit einem symmetrischen Verschlüsselungsverfahren verschlüsselt wird.

[0028] Nach einer Ausführungsform der Erfindung wird ein Verfahren der diskreten logarithmischen Kryptographie (DLC) für die Generierung eines dritten Schlüssels durch das Chipkarten-Terminal und eines vierten Schlüssels durch die Chipkarte verwendet, wobei der vierte Schlüssel nur dann gleich dem dritten Schlüssel ist, wenn die Bedingung PIN' = PIN erfüllt ist.

[0029] Für die Festlegung des dritten Schlüssels kommen im Prinzip beliebige Verfahren der diskreten logarithmischen Kryptographie zur Anwendung, wie sie beispielsweise in der Norm National Institute of Standards and Technology (NIST), NIST Special Publication 800-56A, März, 2007 sowie in Standards for Efficient Cryptography, SEC1: Elliptic Curve Cryptography, Certicom Research, September 20, 2000, Version 1.0, beschrieben sind. Solche Verfahren erfordern die Erzeugung von so genannten Domainparametern zum Zweck der Generierung der identischen dritten und vierten Schlüssel durch das Chipkarten-Terminal bzw. die Chipkarte.

[0030] Nach einer Ausführungsform der Erfindung wird als DLC ein Verfahren der elliptischen Kurvenkryptographie (ECC) eingesetzt, insbesondere Elliptic Curve Diffie-Hellman (ECDH).

[0031] Nach einer Ausführungsform der Erfindung wird die erste Kennung, d. h. die PIN', die in den Chipkarten-Terminal eingegeben wird, wird als so genannter Seed Value für die Ableitung des ersten symmetrischen Schlüssels verwendet. Dadurch wird ein Schlüssel einer größeren Länge erzeugt, als die bei Verwendung der ersten Kennung unmittelbar als Schlüssel der Fall wäre.

[0032] Nach einer Ausführungsform der Erfindung wird auf der Chipkarte eine zweite Kennung, d. h. die PIN, gespeichert, aus der der zweite Schlüssel für die Entschlüsselung des von dem Chipkarten-Terminal initial empfangenen Chiffrats ableitbar ist. Zur Ableitung des zweiten Schlüssels aus der zweiten Kennung kann die zweite Kennung als Seed Value verwendet werden.

[0033] Nach einer Ausführungsform der Erfindung ist nicht die PIN selbst in der Chipkarte gespeichert, sondern nur der zweite Schlüssel. Der zweite Schlüssel ist vorzugsweise in einem nichtflüchtigen geschützten Speicherbereich der Chipkarte gespeichert. Im Unterschied zum Stand der Technik ist also die Speicherung der PIN als Referenzwert in der Chipkarte nicht erforderlich.

[0034] Nach einer Ausführungsform der Erfindung hat die Chipkarte einen Fehlbedienungs-Zähler. Wenn aufgrund einer Fehleingabe der PIN' die ersten und zweiten Kommunikationskanäle nicht übereinstimmen, so inkrementiert bzw. dekrementiert die Chipkarte den Fehlbedienungs-Zähler mit jeder Nachricht, die die Chipkarte auf einem anderen als dem zweiten oder dem vordefinierten Kommunikationskanal empfängt. Solche Nachrichten, die die Chipkarte auf einem anderen als den zweiten oder dem vordefinierten Kommunikationskanal empfängt, werden von der Chipkarte ansonsten ignoriert. Wenn die Anzahl der Fehlbedienungen einen vorgegebenen Schwellwert überschreitet, so wird die Chipkarte insgesamt oder eine bestimmte Chipkartenfunktion, reversibel oder irreversibel gesperrt.

[0035] Nach einer Ausführungsform der Erfindung hat die Chipkarte eine Erstbenutzerfunktion. Die unbenutzte Chipkarte befindet sich in ihrem Erstbenutzungszustand, in dem ein bestimmter Kommunikationsparameter für eine erste Wahl des ersten Kommunikationskanals festgelegt ist. Die Chipkarte geht aus ihrem Erstbenutzungszustand in einen Benutztzustand über, wenn sie zum ersten Mal ein Chipkartenkommando auf diesem ersten Kommunikationskanal empfängt. Für die weitere Verwendung der Chipkarte muss dann seitens des Chipkartenterminals ein anderer Kommunikationsparameter gewählt werden.

[0036] In einem weiteren Aspekt betrifft die Erfindung eine Chipkarte mit Chipkarte mit einer Schnittstelle zur Kommunikation über einen vordefinierten Kommunikationskanal und mehreren weiteren Kommunikationskanälen mit einem Chipkarten-Terminal, Mitteln zur Entschlüsselung eines auf dem vordefinierten Kanal empfangenen Chiffrats, welches mit Hilfe eines ersten symmetrischen Schlüssel verschlüsselt ist, mit Hilfe eines zweiten symmetrischen Schlüssels, wobei die Entschlüsselung zumindest einen Kommunikationsparameter ergibt, wenn eine zuvor in den Chipkarten-Terminal eingegebene erste Kennung zutreffend ist, wobei durch den Kommunikationsparameter einer der weiteren Kommunikationskanäle für die geschützte Kommunikation zwischen der Chipkarte und dem Chipkarten-Terminal eindeutig festgelegt ist.

[0037] In einem weiteren Aspekt betrifft die Erfindung ein Chipkarten-Terminal mit Mitteln zur Eingabe einer ersten Kennung, Mitteln zur Erzeugung eines Chiffrats aus zumindest einem ersten Kommunikationsparameter mit Hilfe eines aus der ersten Kennung abgeleiteten ersten symmetrischen Schlüssels, wobei mit Hilfe des Kommunikationsparameters ein geschützter erster Kommunikationskanal zwischen dem Chipkarten-Terminal und der Chipkarte definierbar ist, und Mitteln zum Senden des Chiffrats über einen vordefinierten Kommunikationskanal an die

Chipkarte.

[0038] Im Weiteren werden Ausführungsformen der Erfindung mit Bezugnahme auf die Zeichnungen näher erläutert. Es zeigen:

[0039] Fig. 1 ein Blockdiagramm einer ersten Ausführungsform einer erfindungsgemäßen Chipkarte und eines Chipkarten-Terminals,

[0040] Fig. 2 ein Flussdiagramm einer Ausführungsform eines erfindungsgemäßen Verfahrens,

[0041] Fig. 3 ein Blockdiagramm einer weiteren Ausführungsform einer erfindungsgemäßen Chipkarte und eines Chipkarten-Terminals,

[0042] Fig. 4 ein Flussdiagramm einer weiteren Ausführungsform eines erfindungsgemäßen Verfahrens.

[0043] In den nachfolgenden Figuren sind einander entsprechende Elemente der verschiedenen Ausführungsformen mit gleichen Bezugszeichen gekennzeichnet.

[0044] Die Fig. 1 zeigt ein Blockdiagramm eines Chipkarten-Terminals **100**. Der Chipkarten-Terminal **100** hat eine Schnittstelle **102** zur Kommunikation mit einer Chipkarte **104**, die eine entsprechende Schnittstelle **106** aufweist. Vorzugsweise sind die Schnittstellen **102** und **106** für eine drahtlose Kommunikation, beispielsweise über Funk, insbesondere nach einem RFID-Verfahren ausgebildet.

[0045] Die Schnittstellen **102** und **106** sind beispielsweise so beschaffen, dass zwischen den Schnittstellen **102**, **106** verschiedene Kommunikationskanäle aufgebaut werden können, wobei sich diese Kommunikationskanäle auf einer physikalischen und/oder logischen Ebene voneinander unterscheiden. Beispielsweise können Kommunikationskanäle unterschiedlicher Übertragungsfrequenzen aufgebaut werden. Es können auch Kommunikationskanäle auf der Basis verschiedener Frequenz-Hopping-Schemata aufgebaut werden. Unter „Frequenz-Hopping" werden hier Frequenzsprung-Verfahren verstanden, wonach die für die Datenübertragung verwendeten Frequenzen nach einem definierten Schema fortlaufend geändert werden.

[0046] Die Schnittstellen **102**, **106** können auch so ausgebildet sein, dass unterschiedliche Kommunikationskanäle mit Hilfe unterschiedlicher Codierungsverfahren und/oder Modulationsverfahren, wie zum Beispiel Frequenzmodulation, Amplitudenmodulation, Phasenmodulation, Pulsweitenmodulation oder anderer Modulationsverfahren aufgebaut werden.

[0047] Die verschiedenen Kommunikationskanäle, die zwischen den Schnittstellen **102** und **106** aufgebaut werden können, werden im Weiteren als die „Menge der Kommunikationskanäle" bezeichnet.

[0048] Einer der Kommunikationskanäle **108** aus der Menge der Kommunikationskanäle ist für die initiale Kommunikation zwischen dem Chipkarten-Terminal **100** und der Chipkarte **104** vordefiniert. Beispielsweise ist der Kommunikationskanal hinsichtlich seiner Übertragungsfrequenz sowie der zu verwendenden Modulations- und Codierungsverfahren vordefiniert.

[0049] Der vordefinierte Kommunikationskanal dient zur Übertragung von einem Chiffrat **110** des zumindest einen Kommunikationsparameters K1 von dem Chipkarten-Terminal **100** zu der Chipkarte **104**, um der Chipkarte **104** mitzuteilen, welcher der Kommunikationskanäle **112** der Menge von Kommunikationskanälen für die nachfolgende Kommunikation mit dem Chipkarten-Terminal **100** verwendet werden soll.

[0050] Der Kommunikationsparameter K1 beinhaltet also eine Angabe, die diesen Kommunikationskanal **112** eindeutig spezifiziert. Diese Angabe kann in Form eines Codeworts erfolgen. In der Chipkarte **104** kann in einem nichtflüchtigen Speicher eine so genannte Lookup-Tabelle gespeichert sein, in der den möglichen Codeworten jeweils eine Spezifizierung einer der Kommunikationskanäle der Menge der Kommunikationskanäle zugeordnet ist.

[0051] Für die Auswahl eines Kommunikationskanals aus der Menge von Kommunikationskanälen können sämtliche mögliche, zwischen den Schnittstellen **102**, **106** aufbaubare Kommunikationskanäle zur Verfügung stehen oder eine Auswahl davon, wobei dann jeder der Kommunikationskanäle der Menge von Kommunikationskanälen, der tatsächlich für die Kommunikation zwischen der Schnittstelle **102**, **106** verwendet werden kann, einem eindeutigen Codewort zugeordnet ist, welches als Kommunikationsparameter **110** von dem Chipkarten-Terminal **100** an die Chipkarte **104** übertragen werden kann.

[0052] Das Chipkarten-Terminal **100** hat eine Nutzerschnittstelle **114**, wie zum Beispiel eine Tastatur oder eine graphische Benutzeroberfläche, über die eine erste Kennung **116** eingegeben werden kann. Diese erste Kennung wird im Weiteren ohne Beschränkung der Allgemeinheit als PIN' bezeichnet.

[0053] Das Chipkarten-Terminal **100** hat zumindest einen Prozessor **118** zur Ausführung eines Anwendungsprogramms **120**. Das Anwendungsprogramm **120** kann die Generierung eines Chipkarten-Kommandos **122** veranlassen, um eine bestimmte Chipkartenfunktion **124** der Chipkarte **104** aufzurufen. Beispielsweise benötigt das Anwendungsprogramm

120 die Chipkartenfunktion **124** für eine Authentizitätsprüfung, für die Generierung einer digitalen Signatur, für die Überprüfung einer Berechtigung, insbesondere einer Zugangsberechtigung, die Vornahme einer finanziellen Transaktion oder dergleichen.

[0054] Der Prozessor **118** dient ferner zur Ausführung der Programminstruktionen eines Kommunikationsmoduls **126**, welches zur Auswahl des Kommunikationskanals **112** aus der Menge der Kommunikationskanäle und damit zur Wahl des Kommunikationsparameters **110** dient. Die Auswahl des Kommunikationsparameters **110** kann nach einem vorgegebenen Schema oder zufällig, insbesondere pseudo-zufällig, erfolgen. Beispielsweise ist in dem Kommunikationsmodul **126** eine Liste von verschiedenen Kommunikationsparametern **110** abgelegt, die zyklisch abgearbeitet wird.

[0055] Der Prozessor **118** dient ferner der Ausführung von Programminstruktionen **128** für eine symmetrische Verschlüsselung der Kommunikationsparameter **110**. Die Verschlüsselung erfolgt mit Hilfe der PIN'. Hierzu können die Programminstruktionen **128** einen Schlüsselgenerator **130** beinhalten.

[0056] Der Schlüsselgenerator **130** kann so ausgebildet sein, dass er aus der PIN' als Seed Value einen ersten symmetrischen Schlüssel generiert, der im Weiteren als S1 bezeichnet wird. Der Schlüssel S1 dient zur symmetrischen Verschlüsselung des von dem Kommunikationsmodul **126** selektierten Kommunikationsparameters K1. Das sich aus der symmetrischen Verschlüsselung mit dem Schlüssel S1 ergebende Chiffrat des Kommunikationsparameters K1 wird über den vordefinierten Kommunikationskanal **108** von der Schnittstelle **102** zu der Schnittstelle **106** übertragen.

[0057] Die Chipkarte **104** hat einen Prozessor **132**, der zur Ausführung der Programminstruktionen eines Kommunikationsmoduls **134** dient. Das Kommunikationsmodul **134** ist zur Verarbeitung des von dem Chipkarten-Terminal **100** gegebenenfalls empfangenen Kommunikationsparameters K1 ausgebildet. Das Kommunikationsmodul **134** kann beispielsweise mit dem Kommunikationsparameter K1 als Schlüssel auf eine Zuordnungstabelle, insbesondere eine lookup Tabelle, zugreiben, um die Parameter des von dem Chipkarten-Terminal **100** selektierten Kommunikationskanals **112** abzufragen, wie zum Beispiel dessen Übertragungsfrequenz und/oder die zu verwendenden Codierungs- und Modulationsverfahren.

[0058] Der Prozessor **132** dient ferner zur Ausführung von Programminstruktionen **136** für die symmetrische Entschlüsselung des Chiffrats **110**, welches die Chipkarte **104** von dem Chipkarten-Terminal **100** empfangen hat. Beispielsweise hat die Chipkarte **104** einen geschützten Speicherbereich **138**, in dem eine zweite Kennung **140** gespeichert ist. Die zweite Kennung wird im Weiteren ohne Beschränkung der Allgemeinheit als PIN bezeichnet. Die PIN wird dem autorisierten Benutzer der Chipkarte mit der Aushändigung der Chipkarte **104** gesondert mitgeteilt, beispielsweise in Form eines so genannten PIN-Briefes.

[0059] Die Programminstruktionen **136** können einen Schlüsselgenerator **142** beinhalten, der die PIN als so genannten Seed Value verwendet, um daraus einen zweiten Schlüssel abzuleiten. Dieser symmetrische zweite Schlüssel wird im Weiteren als S2 bezeichnet.

[0060] Alternativ kann der Schlüssel S2 in dem geschützten Speicherbereich **138** der Chipkarte **104** anstelle der PIN **140** gespeichert sein. Der Schlüsselgenerator **142** sowie eine Speicherung der PIN **140** in der Chipkarte **104** erübrigen sich dann. Im Unterschied zum Stand der Technik muss also auf der Chipkarte **104** nicht unbedingt die PIN **140** als Referenzwert für die Prüfung der Richtigkeit der PIN' **116** gespeichert sein.

[0061] Die Chipkarte **104** kann ferner einen Fehlbedienungs-Zähler **144** aufweisen. Der Fehlbedienungs-Zähler **144** ist so ausgebildet, dass jede Fehlbedienung der Chipkarte **104** gezählt wird. Die Anzahl der Fehlbedienungen wird mit einem vorgegebenen Schwellwert verglichen. Wenn dieser Schwellwert erreicht wird, wird zumindest die Chipkartenfunktion **124**, welcher der Fehlbedienungs-Zähler **144** zugeordnet ist, reversibel oder irreversibel gesperrt.

[0062] Die Chipkarte **104** kann ferner eine Erstbenutzungsfunktion aufweisen. Beispielsweise ist der Erstbenutzungsstatus der Chipkarte **104** durch einen bestimmten Kommunikationsparameter definiert, der einen der Kommunikationskanäle der Menge spezifiziert, der für die erste Benutzung der Chipkarte verwendet werden muss.

[0063] Zur Verwendung der Chipkarte **104** wird wie folgt vorgegangen: Ein Benutzer gibt die PIN' **116** über die Nutzerschnittstelle **114** in den Chipkarten-Terminal **100** ein. Dies kann auf eine entsprechende Anforderung des Anwendungsprogramms **120** hin geschehen. Das Kommunikationsmodul **126** wählt daraufhin einen ersten der möglichen Kommunikationsparameter beispielsweise aus der vorgegebenen Liste der Kommunikationsparameter aus, also den Kommunikationsparameter K1.

[0064] Der Schlüsselgenerator **130** generiert aus der PIN' den Schlüssel S1. Der Kommunikationsparameter K1 wird daraufhin durch Ausführung der Programminstruktionen **128** mit Hilfe des symmetrischen Schlüssels S1 verschlüsselt. Das daraus resultierende Chiffrat **110** des Kommunikationsparameters K1

wird dann über den vordefinierten Kommunikationskanal **108** von der Schnittstelle **102** an die Schnittstelle **106** der Chipkarte **104** gesendet.

[0065] Die Chipkarte **104** leitet erforderlichenfalls den Schlüssel S2 aus der PIN ab oder greift direkt auf den Schlüssel S2 in den geschützten Speicherbereich **138** zu. Mit Hilfe des Schlüssels S2 wird der Versuch einer Entschlüsselung des von dem Chipkarten-Terminal **100** empfangenen Chiffrats **110** des Kommunikationsparameters K1 durch Ausführung der Programminstruktionen **136** von der Chipkarte **104** unternommen.

[0066] Das Ergebnis dieses Entschlüsselungsversuchs ist ein zweiter Kommunikationsparameter, der im Weiteren als K2 bezeichnet wird, und der dem Kommunikationsmodul **134** übergeben wird. Dieser Kommunikationsparameter K2 ist nur dann identisch mit dem Kommunikationsparameter K1, wenn die Bedingung PIN' = PIN erfüllt ist, da nur dann der Schlüssel S1, der für die symmetrische Verschlüsselung verwendet worden ist, gleich dem Schlüssel S2 sein kann, welcher für die symmetrische Entschlüsselung des Chiffrats des Kommunikationsparameters K1 verwendet wurde.

[0067] Durch den Kommunikationsparameter K2 kann ein zweiter Kommunikationskanal **146** definiert sein, indem nämlich das Kommunikationsmodul **134** mit dem Kommunikationsparameter K2 auf seine Zuordnungstabelle zugreift. Dieser zweite Kommunikationskanal **146** ist wiederum nur dann identisch mit dem ersten Kommunikationskanal **112**, wenn die Bedingung PIN' = PIN erfüllt ist.

[0068] Nach der Übertragung des Chiffrats des Kommunikationsparameters K1 über den vordefinierten Kommunikationskanal **108** generiert das Chipkarten-Terminal **100** das Chipkarten-Kommando **122**, welches über den ersten Kommunikationskanal **112** von der Schnittstelle **102** an die Schnittstelle **106** gesendet wird. Die Chipkarte **104** bzw. deren Kommunikationsmodul **134** sind für den Empfang auf den zweiten Kommunikationskanal **146** aufgrund des Kommunikationsparameters K2 eingestellt.

[0069] Wenn der zweite Kommunikationskanal **146** mit dem ersten Kommunikationskanal **112** übereinstimmt, so wird das Chipkarten-Kommando **122** von der Chipkarte **104** verarbeitet und die Chipkartenfunktion **124** wird aufgerufen. Als Ergebnis generiert die Chipkarte **104** eine Antwort auf das Chipkarten-Kommando **122** und überträgt diese Antwort über den ersten Kommunikationskanal **112** zurück an die Chipkarte **100**.

[0070] Wenn hingegen der zweite Kommunikationskanal **146** nicht identisch mit dem ersten Kommunikationskanal **112** ist, so ignoriert die Chipkarte **104** das auf dem ersten Kommunikationskanal **112** empfangene Chipkarten-Kommando und inkrementiert den Fehlbedienungs-Zähler **144**.

[0071] Beispielsweise ist der Kommunikationskanal **108** durch eine Übertragungsfrequenz von 9 GHz definiert, der Kommunikationskanal **112** durch eine Übertragungsfrequenz von 10 GHz und der Kommunikationskanal **146** durch eine Übertragungsfrequenz von 11 GHz, wobei die Übertragungsfrequnzen der Kommunikationskanäle **112** und **146** voneinander abweichen, da die in den Chipkartenterminal **100** eingegebene PIN' nicht gleich der PIN ist. Wenn die Chipkarte **104** in diesem Fall ein Signal auf der Frequnz 10 GHz von dem Chipkartenterminal **100** empfängt, obwohl sie einen Empfang auf der Frequenz 11 GHz erwartet hat, wird dieses Signal ignoriert und der Fehlbedienungszähler wird inkrementiert. Dadurch ist eine implizite Überprüfung der PIN' gegeben, ohne dass die PIN' unmittelbar mit der PIN verglichen werden müsste, und ohne dass die PIN in der Chipkarte gespeichert sein muss.

[0072] Die Fig. 2 zeigt ein entsprechendes Flussdiagramm. In dem Schritt **200** wird die PIN' in dem Chipkarten-Terminal eingegeben. Daraufhin wird in dem Schritt **202** durch den Chipkarten-Terminal **100** der Kommunikationsparameter K1 zur Auswahl eines der Kommunikationskanäle aus der Menge der Kommunikationskanäle festgelegt. In dem Schritt **204** wird der Kommunikationsparameter K1 mit Hilfe der PIN' symmetrisch verschlüsselt. Dies kann so erfolgen, dass aus der PIN' mit Hilfe eines Schlüsselgenerators der symmetrische Schlüssel S1 abgeleitet wird, der dann zur Verschlüsselung des Kommunikationsparameters K1 dient.

[0073] In dem Schritt **206** wird das mit Hilfe des Schlüssels S1 erzeugte Chiffrat des Kommunikationsparameters K1 über einen vordefinierten Kommunikationskanal von dem Chipkarten-Terminal an die Chipkarte übertragen.

[0074] Die Chipkarte **104** unternimmt in dem Schritt **208** den Versuch einer Entschlüsselung des Kommunikationsparameters K1 auf der Basis der PIN. Die zutreffende PIN kann in einem geschützten Speicherbereich der Chipkarte gespeichert sein, und wird zur Ableitung eines symmetrischen Schlüssels S2 verwendet. Alternativ kann auch unmittelbar der Schlüssel S2 in dem geschützten Speicherbereich der Chipkarte gespeichert sein.

[0075] Die Entschlüsselung des Chiffrats des Kommunikationsparameters K1 mit dem Schlüssel S2 hat einen Kommunikationsparameter K2 zum Ergebnis. Durch diesen Kommunikationsparameter K2 kann ein zweiter Kommunikationskanal der Menge definiert sein. Nur wenn die PIN' zutreffend ist, d. h. wenn die Bedingung PIN' = PIN erfüllt ist, sind die durch die

Kommunikationsparameter K1 und K2 spezifizierten Kommunikationskanäle identisch.

[0076] In dem Schritt **210** generiert der Chipkarten-Terminal ein Chipkarten-Kommando und sendet dies über den ersten, durch den Kommunikationsparameter K1 spezifizierten Kommunikationskanal an die Chipkarte (Schritt **212**). In dem Schritt **214** kann die Chipkarte das Chipkarten-Kommando nur dann empfangen, wenn der zweite Kommunikationskanal, auf den die Chipkarte zum Empfang eingerichtet ist, identisch mit dem ersten Kommunikationskanal ist, d. h. wenn die Bedingung PIN' = PIN erfüllt ist. Im gegenteiligen Fall ignoriert die Chipkarte das auf dem ersten Kommunikationskanal empfangene Chiffrat und inkrementiert deren Fehlbedienungs-Zähler.

[0077] Bei dem Kommunikationsparameter K1 kann es sich in einer Ausführungsform der Erfindung um einen öffentlichen Schlüssel des Chipkarten-Terminals handeln. Das Chiffrat dieses öffentlichen Schlüssels, das mit Hilfe des Schlüssels S1 durch symmetrische Verschlüsselung generiert worden ist, wird von dem Chipkarten-Terminal an die Chipkarte übertragen. Die Chipkarte empfängt nur dann den korrekten öffentlichen Schlüssel des Chipkarten-Terminals, wenn wiederum die Bedingung PIN' = PIN erfüllt ist, da nur dann die Entschlüsselung des Chiffrats mit Hilfe des Schlüssels S2 gelingt (vergleiche die Ausführungsform der Fig. 1). Den öffentlichen Schlüssel der Chipkarte kann das Chipkarten-Terminal beispielsweise von einem externen Schlüsselserver über ein Netzwerk, insbesondere das Internet, abfragen.

[0078] Aus dem privaten Schlüssel des Chipkarten-Terminals und dem öffentlichen Schlüssel der Chipkarte kann das Chipkarten-Terminal nach dem Diffie-Hellman-Verfahren einen symmetrischen Schlüssel S3 ableiten. Dementsprechend kann die Chipkarte aus dem öffentlichen Schlüssel des Chipkarten-Terminals und seinem privaten Schlüssel ebenfalls nach dem Diffie-Hellman-Verfahren einen symmetrischen Schlüssel S4 ableiten. Die Schlüssel S3 und S4 sind identisch, wenn die Bedingung PIN' = PIN erfüllt ist.

[0079] Der erste Kommunikationskanal (vergleiche Kommunikationskanal **112** der Fig. 1) ist in dieser Ausführungsform zumindest ergänzend über die symmetrischen Schlüssel S3 = S4 definiert. Das von dem Chipkarten-Terminal an die Chipkarte gesendete Chipkarten-Kommando wird nämlich mit dem symmetrischen Schlüssel S3 verschlüsselt, und kann nur dann von der Chipkarte entschlüsselt, d. h. empfangen werden, wenn sich das Chipkarten-Kommando mit Hilfe des Schlüssels S4 entschlüsseln lässt. Andernfalls wird das Chipkarten-Kommando ignoriert und der Fehlbedienungs-Zähler wird inkrementiert.

[0080] Die Fig. 3 zeigt eine Ausführungsform einer erfindungsgemäßen Chipkarte und eines erfindungsgemäßen Chipkarten-Terminals, wobei ein Verfahren zur diskreten logarithmischen Kryptographie für die Generierung der Schlüssel S3 bzw. S4 zur Anwendung kommt. Ergänzend zu der Ausführungsform gemäß Fig. 1 dient der Prozessor **118** zur Ausführung von Programminstruktionen **148**, durch welche ein so genanntes Key Establishment Scheme für die Generierung des symmetrischen Schlüssels S3 gegeben ist.

[0081] Das Key Establishment Scheme arbeitet nach einem Verfahren der diskreten logarithmischen Kryptographie (DLC), insbesondere der elliptischen Kurvenkryptographie (EEC), vorzugsweise nach einem elliptischen Kurven-Diffie-Hellman-Verfahren (ECDH). Zur Generierung des symmetrischen Schlüssels S3 erzeugen die Programminstruktionen **148** zunächst erste Domainparameter, die im Weiteren als D1 bezeichnet werden.

[0082] Zusätzlich kann das Kommunikationsmodul **126** einen ersten Kanalparameter KA1 erzeugen oder aus einer vorgegebenen Liste auslesen, welcher zum Beispiel die physikalischen Eigenschaften des ersten Kommunikationskanals spezifiziert. Der erste Kanalparameter KA1 entspricht dem Kanalparameter K1 in der Ausführungsform der Fig. 1.

[0083] Die Domainparameter D1 und der oder die Kanalparameter KA1 werden mit Hilfe des Schlüssels S1 durch die Programminstruktionen **128** verschlüsselt. Das aus KA1, D1 mit Hilfe des Schlüssels S1 gewonnene Chiffrat **110** wird über den vordefinierten Kommunikationskanal **108** von der Schnittstelle **102** zu der Schnittstelle **106** übertragen.

[0084] Die Chipkarte **104** entschlüsselt das Chiffrat **110** mit Hilfe des symmetrischen Schlüssels S2. Als Resultat der Entschlüsselung erhält die Chipkarte **104** den zweiten Kanalparameter KA2, der dem Kommunikationsparameter K2 in der Ausführungsform der Fig. 1 entspricht. Ferner erhält die Chipkarte die Domainparameter D2. Der Kanalparameter KA2 wird durch das Kommunikationsmodul **134** verarbeitet, um beispielsweise die physikalische Spezifizierung des zweiten Kommunikationskanals **146** festzustellen.

[0085] Die Chipkarte **104** hat ergänzend zu der Ausführungsform der Fig. 1 Programminstruktionen **150**, die in ihrer Funktionalität den Programminstruktionen **148** entsprechen, und durch die chipkartenseitig das Key Establishment Scheme implementiert wird.

[0086] Seitens des Chipkarten-Terminal wird durch Ausführung der Programminstruktionen **148** aus den Domainparametern D1 der symmetrische Schlüssel S3 abgeleitet, der in einem Speicher **152** des Chipkarten-Terminals **100** abgelegt wird. Dementspre-

chend wird durch Ausführung der Programminstruktionen **150** seitens der Chipkarte **104** aus den Domainparametern D2 ein symmetrischer Schlüssel S4 abgeleitet, der in einen Speicher **154** der Chipkarte **104** abgelegt wird.

[0087] Das Chipkarten-Kommando **122** wird vor seiner Versendung durch den Chipkarten-Terminal mit dem symmetrischen Schlüssel S3 verschlüsselt und dann über den durch die Kanalparameter KA1 spezifizierten ersten Kommunikationskanal **112** übertragen. Ein Empfang des Chipkarten-Kommandos **122** durch die Chipkarte **104** ist nur möglich, wenn sowohl KA2 = KA1 und D2 = D1 ist, was wiederum nur dann möglich ist, wenn die Bedingung PIN' = PIN erfüllt ist.

[0088] Von besonderem Vorteil bei dieser Ausführungsform ist, dass die Übertragung der Domainparameter D1 über den vordefinierten Kommunikationskanal **108** durch einen Dritten nicht ausgespäht werden kann, da die Übertragung der Domainparameter D1 in einer verschlüsselten Form erfolgt.

[0089] Die Fig. 4 zeigt ein entsprechendes Flussdiagramm. In dem Schritt **400** wird eine PIN' in das Chipkarten-Terminal durch einen Benutzer eingegeben. Aus der PIN' wird der symmetrische Schlüssel S1 abgeleitet.

[0090] In dem Schritt **402** wird das Key Establishment Scheme gestartet. Daraufhin wird in dem Schritt **404** ein Satz Domainparameter D1 erzeugt. Mit Hilfe der Domainparameter D1 wird der symmetrische Schlüssel S3 durch das Chipkarten-Terminal generiert. Ferner werden in dem Schritt **406** durch das Chipkarten-Terminal der Kanalparameter KA1 generiert oder aus einer vorgegebenen Liste ausgelesen.

[0091] In dem Schritt **408** werden die Domainparameter D1 und/oder die Kanalparameter KA1 mit dem Schlüssel S1 verschlüsselt. Beispielsweise werden die Domainparameter D1 und die Kanalparameter KA1 aneinander gehängt, woraus ein einziger Kommunikationsparameter resultiert, der dann mit dem Schlüssel S1 verschlüsselt wird. Alternativ werden nur die Domainparameter D1 oder nur die Kanalparameter KA1 oder eine jeweilige Teilmenge der Domain- und/oder Kanalparameter mit dem Schlüssel S1 verschlüsselt. Das aus der Verschlüsselung mit dem Schlüssel S1 resultierende Chiffrat sowie gegebenenfalls verbleibende unverschlüsselten Domain- und/oder Kanalparameter werden in dem Schritt **410** von dem Chipkarten-Terminal an die Chipkarte über den vordefinierten Kanal (vergleiche Kommunikationskanal **108** der Fig. 1 und Fig. 3) übertragen.

[0092] In dem Schritt **412** versucht die Chipkarte das Chiffrat mit Hilfe des Schlüssels S2 zu entschlüsseln. Daraus erhält die Chipkarte **104** die Kanalparameter KA2 und die Domainparameter D2. Aus den Domainparametern D2 leitet die Chipkarte **104** den Schlüssel S4 ab.

[0093] In dem Schritt **414** generiert das Chipkarten-Terminal **100** ein Chipkarten-Kommando, welches mit dem Schlüssel S3 verschlüsselt wird (Schritt **416**), um dieses über den durch die Kanalparameter KA1 definierten ersten Kommunikationskanal zu übertragen (vergleiche Kommunikationskanal **112** in den Ausführungsformen der Fig. 1 und Fig. 3). Das Chipkarten-Terminal **100** versendet das Chipkarten-Kommando in dem Schritt **418**.

[0094] Ein korrekter Empfang dieses Chiffrats durch die Chipkarte ist in dem Schritt **420** nur dann möglich, wenn der zweite Kommunikationskanal **146** mit dem ersten Kommunikationskanal **112** übereinstimmt, d. h. wenn KA2 = KA1 ist, und wenn außerdem eine Entschlüsselung des Chipkarten-Kommandos mit dem Schlüssel S4 möglich ist, d. h. wenn S4 = S3 ist. Die Bedingungen KA2 = KA1 und S4 = S3 können aber nur dann erfüllt sein, wenn die korrekte PIN' durch den Benutzer in das Chipkarten-Terminal eingegeben worden ist, d. h. wenn PIN' = PIN ist.

Bezugszeichenliste

100	Chipkarten-Terminal
102	Schnittstelle
104	Chipkarte
106	Schnittstelle
108	vordefinierter Kommunikationskanal
110	Kommunikationsparameter
112	erster Kommunikationskanal
114	Nutzerschnittstelle
116	PIN'
118	Prozessor
120	Anwendungsprogramm
122	Chipkarten-Kommando
124	Chipkartenfunktion
126	Kommunikationsmodul
128	Programminstruktionen
130	Schlüsselgenerator
132	Prozessor
134	Kommunikationsmodul
136	Programminstruktionen
138	geschützter Speicherbereich
140	PIN
142	Schlüsselgenerator
144	Fehlbedienungs-Zähler
146	zweiter Kommunikationskanal
148	Programminstruktionen
150	Programminstruktionen
152	Speicher
154	Speicher

Patentansprüche

1. Verfahren zum Schutz einer Chipkarte (**104**) gegen unberechtigte Benutzung mit folgenden

Schritten:
– Eingabe einer ersten Kennung (**116**) in einen Chipkarten-Terminal (**100**),
– Erzeugung eines Chiffrats aus zumindest einem ersten Kommunikationsparameter (K1; KA1, D1) mit Hilfe eines aus der ersten Kennung abgeleiteten ersten symmetrischen Schlüssels (S1), wobei mit Hilfe des Kommunikationsparameters ein geschützter erster Kommunikationskanal (**112**) zwischen dem Chipkarten-Terminal und der Chipkarte definierbar ist,
– Übertragung des Chiffrats über einen vordefinierten Kommunikationskanal (**108**) von dem Chipkarten-Terminal an die Chipkarte,
– Versuch einer Entschlüsselung des Chiffrats mit Hilfe eines zweiten symmetrischen Schlüssels (S2) durch die Chipkarte, wobei das Resultat der Entschlüsselung nur dann der erste Kommunikationsparameter ist, wenn der erste symmetrische Schlüssel dem zweiten symmetrischen Schlüssel gleicht, sodass der geschützte erste Kommunikationskanal nur dann zwischen dem Chipkarten-Terminal und der Chipkarte definierbar ist, wenn die erste Kennung zutreffend ist.

2. Verfahren nach Anspruch 1, wobei es sich bei dem ersten Kommunikationsparameter um die Angabe einer Übertragungsfrequenz, eines Frequenz-Hopping-Schemas, eines Codierungsverfahrens und/oder eines Modulationsverfahrens handelt.

3. Verfahren nach Anspruch 1, wobei es sich bei dem ersten Kommunikationsparameter um einen öffentlichen Schlüssel des Chipkarten-Terminals handelt, wobei die Chipkarte im Fall, dass die Entschlüsselung des Chiffrats gelingt, aus dem öffentlichen Schlüssel nach dem Diffie-Hellman(DH)-Verfahren einen weiteren symmetrischen Schlüssel (S4) zur Verschlüsselung der Kommunikation zwischen dem Chipkarten-Terminal und der Chipkarte ableitet, wobei durch die Verschlüsselung mit dem weiteren symmetrischen Schlüssel der erste Kommunikationskanal definiert ist.

4. Verfahren nach Anspruch 1, wobei es sich bei dem ersten Kommunikationsparameter um einen ersten Domainparameter (D1) für die Durchführung eines diskreten logarithmischen kryptographischen Verfahrens zur Erzeugung eines dritten symmetrischen Schlüssels (S3) durch das Chipkarten-Terminal eines vierten symmetrischen Schlüssels (S4) durch die Chipkarte und handelt, wobei die dritten und vierten Schlüssel identisch sind, wenn die erste Kennung zutreffend ist, wobei die dritten und vierten symmetrische Schlüssel zur Verschlüsselung der Kommunikation zwischen dem Chipkarten-Terminal und der Chipkarte über den geschützten ersten Kommunikationskanal vorgesehen sind.

5. Verfahren nach Anspruch 4, wobei es sich bei dem diskreten logarithmischen kryptographischen Verfahren um ein elliptische Kurven kryptographisches Verfahren handelt.

6. Verfahren nach Anspruch 4 oder 5, wobei es sich bei dem diskreten logarithmischen kryptographischen Verfahren um ein elliptisches Kurven Diffie-Hellman-Verfahren handelt.

7. Verfahren nach einem der vorhergehenden Ansprüche, wobei die erste Kennung als Seed Value für die Ableitung des ersten symmetrischen Schlüssels durch das Chipkarten-Terminal verwendet wird.

8. Verfahren nach einem der vorhergehenden Ansprüche, wobei auf der Chipkarte eine zweite Kennung (**140**) gespeichert ist, aus der der zweite Schlüssel ableitbar ist.

9. Verfahren nach einem der vorhergehenden Ansprüche, wobei der zweite Schlüssel in einem geschützten nicht-volatilen Speicherbereich der Chipkarte gespeichert ist.

10. Verfahren nach einem der vorhergehenden Ansprüche, wobei das Resultat der Entschlüsselung ein nicht zutreffender zweiter Kommunikationsparameter (K2; D2, KA2) ist, wenn die erste Kennung nicht zutreffend ist, wobei durch den zweiten Kommunikationsparameter ein nicht zutreffender zweiter Kommunikationskanal (**146**) durch die Chipkarte definierbar ist, mit folgenden weiteren Schritten:
– Sendung eines Chipkarten-Kommandos (**122**) von dem Chipkarten-Terminal an die Chipkarte auf dem geschützten ersten Kommunikationskanal,
– Ignorierung des Chipkarten-Kommandos durch die Chipkarte und Reduzierung der Anzahl der verbleibenden Fehlbedienungen, wobei die Chipkarte oder eine Chipkartenfunktion der Chipkarte bei Überschreitung einer vorgegebenen Anzahl von Fehlbedienungen gesperrt wird.

11. Chipkarte mit:
– einer Schnittstelle (**106**) zur Kommunikation über einen vordefinierten Kommunikationskanal (**108**) und mehreren weiteren Kommunikationskanälen (**112**, **146**, ...) mit einem Chipkarten-Terminal (**100**),
– Mitteln (**132**, **136**) zur Entschlüsselung eines auf dem vordefinierten Kanal empfangenen Chiffrats, welches mit Hilfe eines ersten symmetrischen Schlüssel verschlüsselt ist, mit Hilfe eines zweiten symmetrischen Schlüssels (S2), wobei die Entschlüsselung zumindest einen Kommunikationsparameter ergibt (K2; KA2, D2), wenn eine zuvor in den Chipkarten-Terminal eingegebene erste Kennung (**116**) zutreffend ist, wobei durch den Kommunikationsparameter einer der weiteren Kommunikationskanäle für die geschützte Kommunikation zwischen der Chipkarte und dem Chipkarten-Terminal eindeutig festgelegt ist,
dadurch gekennzeichnet, dass es sich bei dem Kom-

munikationsparameter um die Angabe einer Übertragungsfrequenz, eines Frequenz-Hopping-Schemas, eines Codierungsverfahrens und/oder eines Modulationsverfahrens handelt.

12. Chipkarte nach Anspruch 11, mit Mitteln (**150**) zur Durchführung eines diskreten logarithmischen Verschlüsselungsverfahrens zur Erzeugung des weiteren symmetrischen Schlüssels (S4), wobei der weitere symmetrische Schlüssel zur symmetrischen Verschlüsselung der Kommunikation zwischen dem Chipkarten-Terminal und der Chipkarte über den festgelegten Kommunikationskanal (**112**) vorgesehen ist.

13. Chipkarte nach einem der vorhergehenden Ansprüche 11 bis 12, mit einem nicht flüchtigen geschützten Speicherbereich zur Speicherung einer zweiten Kennung (**140**), aus der der zweite Schlüssel ableitbar ist.

14. Chipkarte nach einem der vorhergehenden Ansprüche 11 bis 13, mit einem geschützten nicht-flüchtigen Speicherbereich zur Speicherung des zweiten Schlüssels.

15. Chipkarte nach einem der vorhergehenden Ansprüche 11 bis 14, mit einem Fehlbedienungs-Zähler (**144**) zur Sperrung der Chipkarte, wenn die Anzahl der Fehlbedienungen einen vorgegebenen Schwellwert erreicht hat, wobei eine von der Chipkarte empfangene Nachricht, die auf einem der weiteren Kommunikationskanäle, welcher nicht der festgelegt Kommunikationskanal ist, an die Chipkarte gesendet wird, als Fehlbedienung gezählt wird.

16. Chipkarte nach einem der vorhergehenden Ansprüche 11 bis 15, wobei es sich um ein Dokument, insbesondere ein Wert- oder Sicherheitsdokument, um eine Ausweiskarte, ein Zahlungsmittel, eine Signaturkarte oder dergleichen handelt.

17. Chipkarte nach einem der vorhergehenden Ansprüche 11 bis 16, mit einer Erstbenutzerfunktion, wobei in einem Erstbenutzungszustand, ein bestimmter Kommunikationsparameter für eine erste Wahl des ersten Kommunikationskanals festgelegt ist, und wobei die Chipkarte aus ihrem Erstbenutzungszustand in einen Benutztzustand übergeht, wenn sie zum ersten Mal ein Chipkartenkommando (**122**) auf diesem ersten Kommunikationskanal empfängt.

18. Chipkarten-Terminal mit:
– Mitteln (**114**) zur Eingabe einer ersten Kennung (**116**),
– Mitteln zur Erzeugung eines Chiffrats aus zumindest einem ersten Kommunikationsparameter (K1; KA1, D1) mit Hilfe eines aus der ersten Kennung abgeleiteten ersten symmetrischen Schlüssels (S1), wobei mit Hilfe des Kommunikationsparameters ein geschützter erster Kommunikationskanal (**112**) zwischen dem Chipkarten-Terminal und der Chipkarte (**104**) definierbar ist,
– Mitteln zum Senden des Chiffrats über einen vordefinierten Kommunikationskanal (**108**) an die Chipkarte.

19. Chipkarten-Terminal nach Anspruch 18, wobei es sich bei dem ersten Kommunikationsparameter um die Angabe einer Übertragungsfrequenz, eines Frequenz-Hopping-Schemas, eines Codierungsverfahrens und/oder eines Modulationsverfahrens handelt.

20. Chipkarten-Terminal nach Anspruch 18, mit Mitteln (**148**) zur Erzeugung von Domainparametern (D1) für die Durchführung eines diskreten logarithmischen kryptographischen Verfahrens für die Ableitung eines weiteren symmetrischen Schlüssels (S3) zur Verschlüsselung der Kommunikation zwischen dem Chipkarten-Terminal und der Chipkarte, wobei der erste Kommunikationsparameter die Domainparameter angibt.

Es folgen 4 Blatt Zeichnungen

Anhängende Zeichnungen

Fig. 1

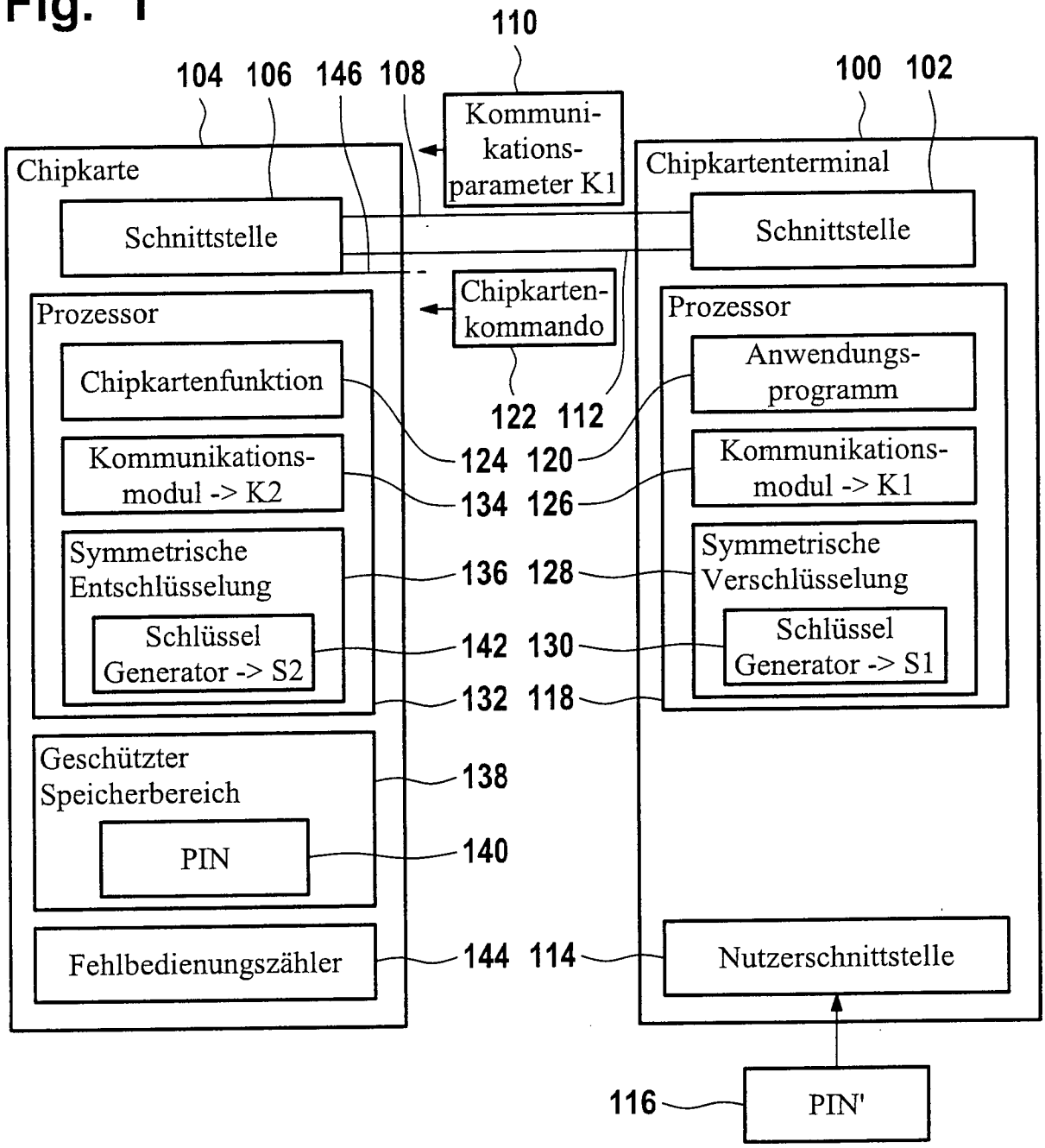


Fig. 2

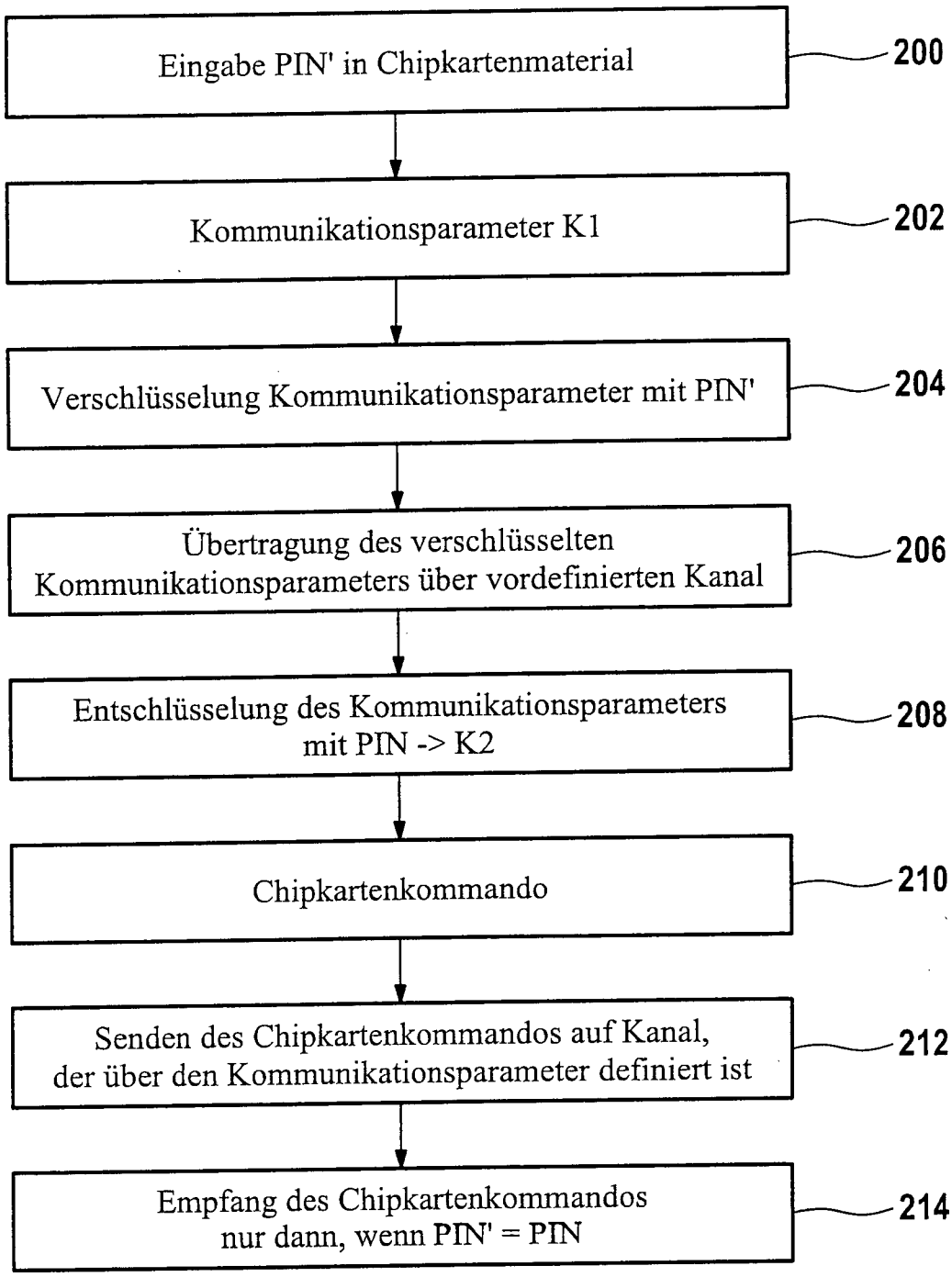

Eingabe PIN' in Chipkartenmaterial
200
Kommunikationsparameter K1
202
Verschlüsselung Kommunikationsparameter mit PIN'
204
Übertragung des verschlüsselten Kommunikationsparameters über vordefinierten Kanal
206
Entschlüsselung des Kommunikationsparameters mit PIN -> K2
208
Chipkartenkommando
210
Senden des Chipkartenkommandos auf Kanal, der über den Kommunikationsparameter definiert ist
212
Empfang des Chipkartenkommandos nur dann, wenn PIN' = PIN
214

Fig. 3

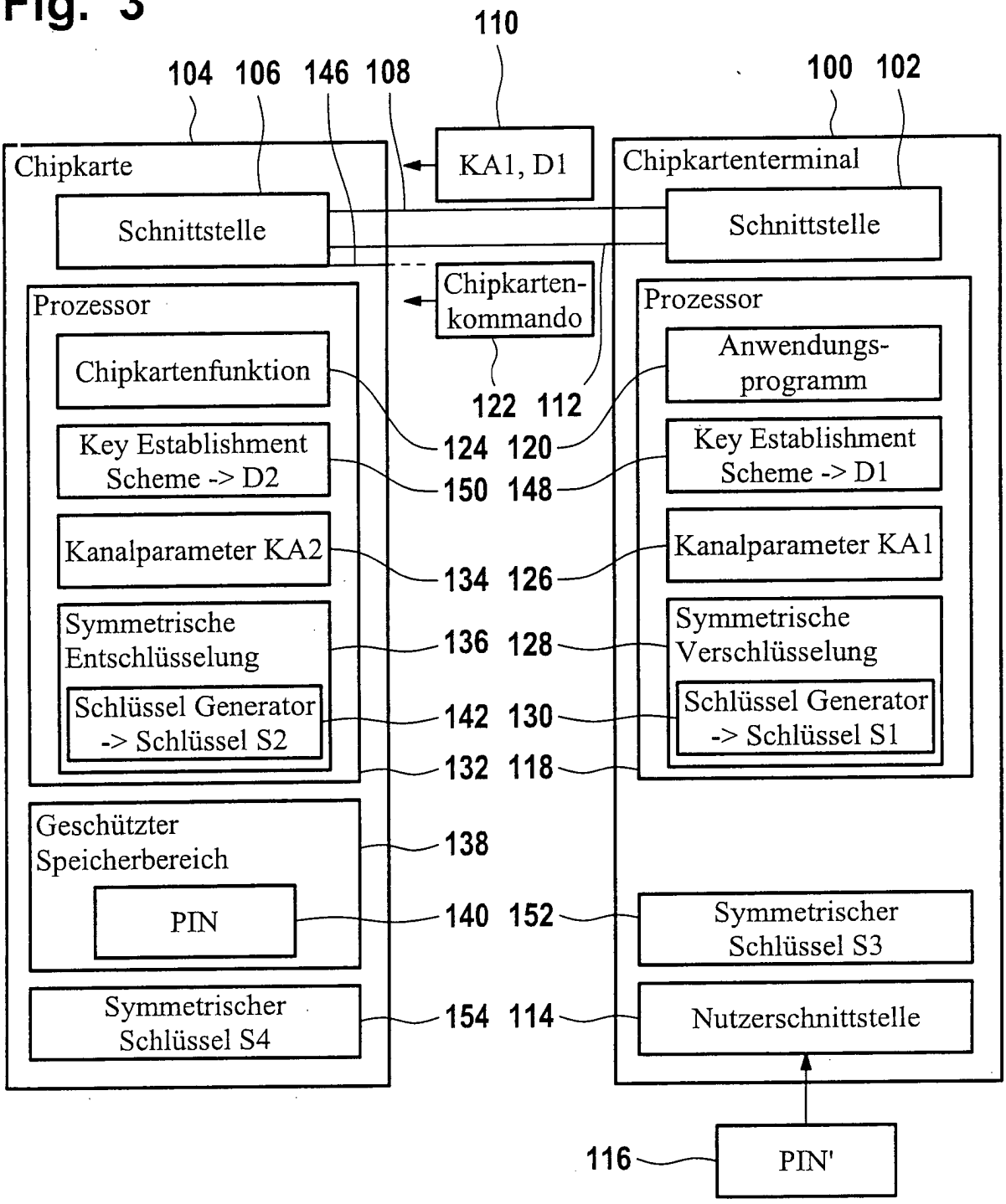
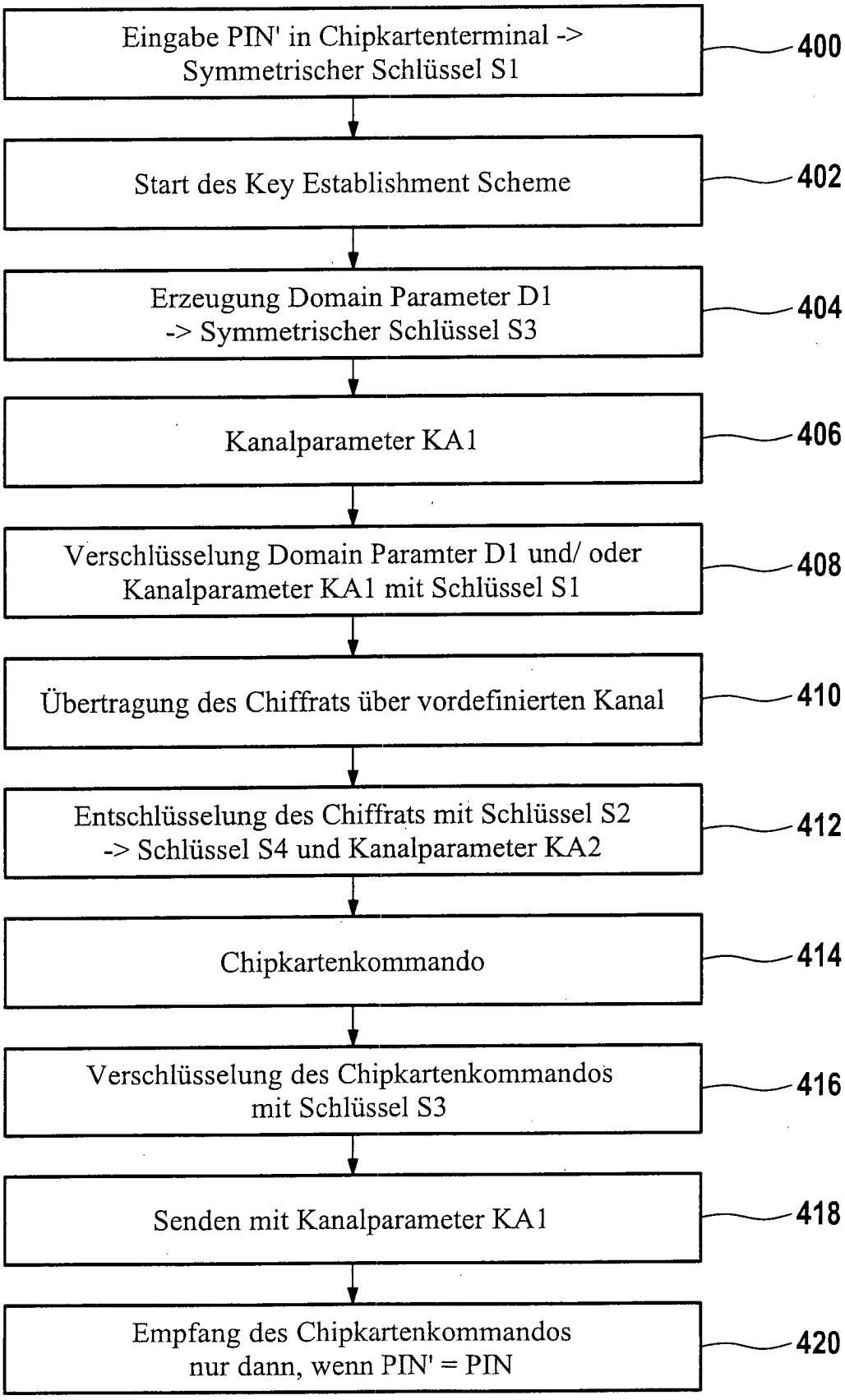

110
104
106
146
108
100
102
Chipkarte
KA1, D1
Chipkartenterminal
Schnittstelle
Schnittstelle
Chipkarten-
kommando
Prozessor
Prozessor
Chipkartenfunktion
Anwendungs-
programm
122
112
Key Establishment
Scheme -> D2
124
120
Key Establishment
Scheme -> D1
150
148
Kanalparameter KA2
Kanalparameter KA1
134
126
Symmetrische
Entschlüsselung
136
128
Symmetrische
Verschlüsselung
Schlüssel Generator
-> Schlüssel S2
142
130
Schlüssel Generator
-> Schlüssel S1
132
118
Geschützter
Speicherbereich
138
PIN
140
152
Symmetrischer
Schlüssel S3
Symmetrischer
Schlüssel S4
154
114
Nutzerschnittstelle
116
PIN'

Fig. 4


Eingabe PIN' in Chipkartenterminal -> Symmetrischer Schlüssel S1
400
Start des Key Establishment Scheme
402
Erzeugung Domain Parameter D1 -> Symmetrischer Schlüssel S3
404
Kanalparameter KA1
406
Verschlüsselung Domain Paramter D1 und/ oder Kanalparameter KA1 mit Schlüssel S1
408
Übertragung des Chiffrats über vordefinierten Kanal
410
Entschlüsselung des Chiffrats mit Schlüssel S2 -> Schlüssel S4 und Kanalparameter KA2
412
Chipkartenkommando
414
Verschlüsselung des Chipkartenkommandos mit Schlüssel S3
416
Senden mit Kanalparameter KA1
418
Empfang des Chipkartenkommandos nur dann, wenn PIN' = PIN
420