(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
3. Juni 2004 (03.06.2004)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2004/046897 A1

(51) Internationale Patentklassifikation[7]: G06F 1/00, G07F 7/10

(21) Internationales Aktenzeichen: PCT/EP2003/012249

(22) Internationales Anmeldedatum:
3. November 2003 (03.11.2003)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
102 51 265.5 4. November 2002 (04.11.2002) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **GIESECKE & DEVRIENT GMBH** [DE/DE]; Prinzregentenstrasse 159, 81677 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **WEIKMANN, Franz** [DE/DE]; Einsteinstrasse 131, 81675 München (DE). **JOHNSON, Eric** [US/DE]; Gaissacherstrasse 7, 81371 München (DE).

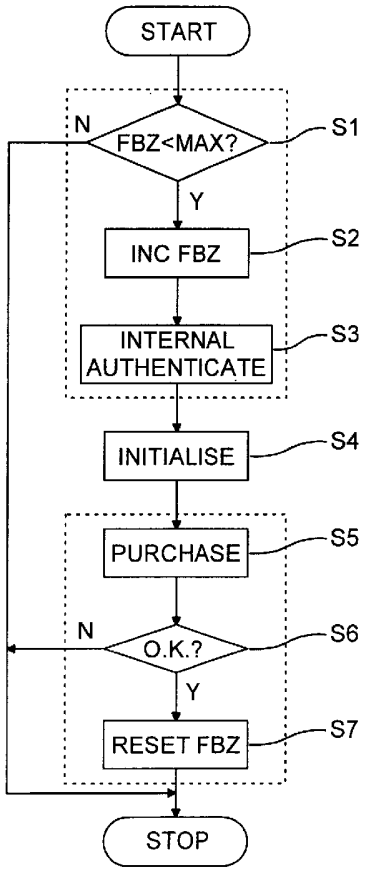
(74) Anwalt: **KLUNKER, SCHMITT-NILSON, HIRSCH**; Winzererstrasse 106, 81797 München (DE).

(81) Bestimmungsstaaten *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

[Fortsetzung auf der nächsten Seite]

(54) **Title:** METHOD FOR THE PROTECTION OF A PORTABLE DATA CARRIER

(54) **Bezeichnung:** VERFAHREN ZUM SCHUTZ EINES TRAGBAREN DATENTRÄGERS



(57) **Abstract:** The invention relates to a method for protecting a portable data carrier, according to which a misoperation counter (FBZ) is provided for detecting the number of calls for an action of the data carrier. Taking a specific action is authorized only if the misoperation counter (FBZ) lies below a predefined threshold value (MAX). The inventive method is characterized by the fact that the misoperation counter (FBZ) is associated with several actions of the data carrier, the misoperation counter (FBZ) being incremented when there is a call for a first action while said misoperation counter (FBZ) is reset when a second action is successfully taken.

(57) **Zusammenfassung:** Die Erfindung betrifft ein Verfahren zum Schutz eines tragbaren Datenträgers, wobei ein Fehlbedienungszähler (FBZ) vorgesehen ist, mit dem die Anzahl der Aufrufe einer Aktion des Datenträgers erfasst wird und wobei eine Durchführung der Aktion nur dann zugelassen wird, wenn der Fehlbedienungszähler (FBZ) unterhalb eines vorgebbaren Schwellwerts (MAX) liegt. Das erfindungsgemässe Verfahren zeichnet sich dadurch aus, dass der Fehlbedienungszähler (FBZ) mehreren Aktionen des Datenträgers zugeordnet wird, indem ein Inkrementieren des Fehlbedienungszählers (FBZ) bei einem Aufruf einer ersten Aktion und ein Rücksetzen des Fehlbedienungszählers (FBZ) bei einer erfolgreichen Durchführung einer zweiten Aktion erfolgt.

WO 2004/046897 A1

(84) **Bestimmungsstaaten** *(regional)*: ARIPO-Patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *mit internationalem Recherchenbericht*

— *vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Verfahren zum Schutz eines tragbaren Datenträgers

Die Erfindung betrifft ein Verfahren zum Schutz eines tragbaren Datenträgers gemäß dem Oberbegriff des Anspruchs 1.

In tragbaren Datenträgern sind häufig geheime Daten gespeichert und/oder geheime Algorithmen implementiert. Diese können beispielsweise dazu verwendet werden, den Datenträger gegenüber einem Endgerät als echt auszuweisen, d. h. eine Authentifizierung des Datenträgers durchzuführen. Weiterhin werden die geheimen Daten bzw. die geheimen Algorithmen für eine Authentifizierung des Endgeräts durch den Datenträger benötigt. Schließlich können die geheimen Daten bzw. Algorithmen zur Prüfung einer Geheimzahl oder eines biometrischen Merkmals herangezogen werden, um festzustellen, ob ein Benutzer zur Verwendung des Datenträgers berechtigt ist, d. h. es wird eine Authentifizierung des Benutzers durchgeführt. Um ein Ausspähen der beim Authentifizierungsvorgang eingesetzten geheimen Daten oder Algorithmen zu verhindern, ist es bereits bekannt, die Anzahl der Authentifizierungsversuche durch einen Fehlbedienungszähler zu begrenzen. Der Fehlbedienungszähler wird bei jedem Authentifizierungsversuch inkrementiert und bei einem erfolgreichen Authentifizierungsversuch zurückgesetzt. Überschreitet der Fehlbedienungszähler einen Schwellwert, so wird kein weiterer Authentifizierungsversuch mehr zugelassen.

Aus der DE 43 39 460 C1 ist ein Challenge-and-Response-Verfahren zur Authentifizierung bekannt, die im Rahmen einer Aufladung eines Wertespeichers eines tragbaren Datenträgers durchgeführt wird. Dabei wird im Datenträger eine Sperre eingerichtet, die nur durch Verändern eines Fehlerzählerstandes aufgehoben werden kann. Danach wird der Fehlerzählerstand geändert und damit die Sperre aufgehoben. Mittels einer Zufallszahl eines Endgeräts und mittels geheimer Schlüsseldaten werden sowohl im Endgerät als auch im Datenträger Authentifikationsparameter ermittelt und im Datenträ-

ger miteinander verglichen. Bei einer Übereinstimmung wird die Sperrvorrichtung deaktiviert, so dass der Wertespeicher wieder aufladbar ist und der Fehlerzähler rücksetzbar ist.

Der Erfindung liegt die Aufgabe zugrunde, den Sicherheitsstandard bei tragbaren Datenträgern weiter zu erhöhen und insbesondere den unbefugten Aufruf von kryptographischen Funktionen einzuschränken.

Diese Aufgabe wird durch ein Verfahren mit der Merkmalskombination des Anspruchs 1 gelöst.

Die Erfindung geht aus von einem Verfahren zum Schutz eines tragbaren Datenträgers, wobei ein Fehlbedienungszähler vorgesehen ist, mit dem die Anzahl der Aufrufe einer Aktion des Datenträgers erfasst wird und wobei eine Durchführung der Aktion nur dann zugelassen wird, wenn der Fehlbedienungszähler unterhalb eines vorgebbaren Schwellwerts liegt.

Weiterhin wird bei der Erfindung von der Erkenntnis Gebrauch gemacht, dass von einem tragbaren Datenträger in der Regel auch Aktionen durchgeführt werden, die nicht auf die übliche Weise direkt mit einem Fehlbedienungszähler abgesichert werden können, bei deren beliebig häufiger Ausführung aber dennoch die Gefahr einer Preisgabe geheimer Daten oder Algorithmen besteht. Dies rührt daher, dass für den Einsatz eines Fehlbedienungszählers im herkömmlichen Sinn nur Aktionen in Frage kommen, bei deren Durchführung Daten auf ihre Korrektheit geprüft werden. Abhängig vom Ergebnis der Prüfung wird der bei jedem Aufruf der Aktion inkrementierte Fehlbedienungszähler zurückgesetzt oder nicht. Die auf herkömmliche Weise mit einem Fehlbedienungszähler abgesicherten Aktionen sind zwar in der Regel besonders kritisch im Hinblick auf ein potentielles Ausspähen, da

von ihnen beispielsweise die weitere Durchführung der Anwendung oder der Zugriff auf Daten abhängt. Es sind aber keineswegs die einzigen Aktionen, bei deren Ausführung geheime Daten oder Algorithmen potentiell ausgespäht werden können, da auch bei anderen Aktionen, die nicht auf herkömmliche Weise mit einem Fehlbedienungszähler abgesichert werden können, beispielsweise Zufallszahlen erzeugt oder Verschlüsselungen von Informationen durchgeführt werden. Bei einer beliebig häufigen Wiederholung dieser ungesicherten Aktionen könnte beispielsweise versucht werden, Rückschlüsse auf die verwendeten Prozeduren zur Generierung der Zufallszahlen oder auf die verwendeten Schlüssel bzw. Verschlüsselungsalgorithmen zu ziehen. Um dies zu verhindern, wird der Fehlbedienungszähler erfindungsgemäß mehreren Aktionen des Datenträgers zugeordnet, indem ein Inkrementieren des Fehlbedienungszählers bei einem Aufruf einer ersten Aktion und ein Rücksetzen des Fehlbedienungszählers bei einer erfolgreichen Durchführung einer zweiten Aktion erfolgt. Dies hat den Vorteil, dass sich beliebige Aktionen des Datenträgers mit einem Fehlbedienungszähler gegen fortwährend wiederholtes Aufrufen absichern lassen. Dabei ist es insbesondere vorteilhaft, dass für den Einsatz der Erfindung bei einem Datenträger keine Veränderung der Spezifikation erforderlich ist.

Beim erfindungsgemäßen Verfahren können die erste Aktion und die zweite Aktion in eine Sequenz eingebunden sein, so dass bei einem ordnungsgemäßen Betrieb des Datenträgers bei einer Ausführung der ersten Aktion stets auch die zweite Aktion ausgeführt wird. Dadurch wird sichergestellt, dass bei einem ordnungsgemäßen Betrieb des Datenträgers nach einem Inkrementieren des Fehlbedienungszählers stets die Möglichkeit besteht, den Fehlbedienungszähler zurückzusetzen. Zwischen der ersten Aktion und der zweiten Aktion kann wenigstens eine weitere Aktion ausgeführt werden.

Dies hat den Vorteil, dass die weitere Aktion ebenfalls mit dem Fehlbedienungszähler abgesichert werden kann.

In einem bevorzugten Ausführungsbeispiel wird zu Beginn der ersten Aktion überprüft, ob der Fehlbedienungszähler unterhalb eines Schwellwerts liegt und eine Durchführung der ersten Aktion nur dann zugelassen, wenn die Überprüfung ein positives Ergebnis liefert. Weiterhin wird der Fehlbedienungszähler vorzugsweise zu Beginn der ersten Aktion inkrementiert. Die Inkrementierung kann dabei unmittelbar vor oder unmittelbar nach der Überprüfung erfolgen. Die frühzeitige Ausführung dieser Sicherheitsmaßnahmen ermöglicht einen besonders guten Schutz vor Manipulationen.

Mit dem erfindungsgemäßen Verfahren werden insbesondere erste Aktionen abgesichert, die so ausgebildet sind, dass bei deren Durchführung geheime Daten verarbeitet und/oder geheime Algorithmen angewendet werden. Die erste Aktion kann beispielsweise in einer Erzeugung einer Zufallszahl, einer Verschlüsselung einer Zeichenfolge, einer Berechnung einer Prüfsumme oder einer Erzeugung einer digitalen Signatur bestehen. Dabei ist die erste Aktion in der Regel so ausgebildet, dass bei deren Durchführung vom Datenträger nicht geprüft wird, ob eine autorisierte Benutzung des Datenträgers vorliegt. Die zweite Aktion ist dagegen in der Regel so ausgebildet, dass bei deren Durchführung eine dem Datenträger übermittelte Information geprüft wird und der Fehlbedienungszähler zurückgesetzt wird, wenn die Prüfung erfolgreich verläuft.

Die Erfindung wird im folgenden anhand der in der Zeichnung dargestellten Ausführungsbeispiele näher erläutert. Die Ausführungsbeispiele beziehen sich jeweils auf eine Anwendungssituation, bei der einem tragbaren Datenträger von einem Endgerät Kommandos übermittelt werden. Der Datenträ-

ger, der beispielsweise als Chipkarte ausgebildet sein kann, arbeitet die Kommandos ab und übermittelt gegebenenfalls ein Ergebnis an das Endgerät. Um ein Ausspähen der bei der Abarbeitung der Kommandos eingesetzten Daten und/oder Algorithmen zu verhindern, wird die Ausführung von in dieser Hinsicht kritischen Kommandos mittels des erfindungsgemäßen Verfahrens durch einen Fehlbedienungszähler abgesichert. Dies wird an Hand einiger typischer Kommandosequenzen beispielhaft erläutert.

Es zeigen

Fig. 1 ein Flußdiagramm für eine Kommandosequenz, die mit dem erfindungsgemäßen Verfahren abgesichert wird,

Fig. 2 ein Flußdiagramm für eine weitere Kommandosequenz, die ebenfalls mit dem erfindungsgemäßen Verfahren abgesichert wird und

Fig. 3 ein Flußdiagramm für eine nochmals andere Kommandosequenz, die wiederum mit dem erfindungsgemäßen Verfahren abgesichert wird.

In Fig. 1 ist ein Flußdiagramm dargestellt, anhand dessen die Absicherung eines Kommandos erläutert wird, das als INTERNAL AUTHENTICATE bezeichnet wird. Bei der Durchführung dieses Kommandos verschlüsselt der Datenträger eine Zufallszahl oder eine Zeichenfolge, die ihm zu diesem Zweck vom Endgerät als Klartext übermittelt wurde, und gibt das Ergebnis der Verschlüsselung an das Endgerät aus. Ein potentieller Angreifer könnte dem Datenträger dieses Kommando ausführen lassen und dadurch den zu einem vorgegebenen Klartext zugehörigen verschlüsselten Text ermitteln. Durch eine fortwährende Ausführung des Kommandos mit einer systematischen Variation des Klartextes ließen sich aus dem jeweils ermittelten ver-

schlüsselten Text möglicherweise Rückschlüsse auf das Verschlüsselungsverfahren und den verwendeten Schlüssel ziehen. Wie groß die Erfolgsaussichten eines derartigen Angriffs sind, hängt unter anderem von der Stärke des Verschlüsselungsverfahrens, von der verwendeten Schlüssellänge und von der Anzahl der Aufrufe des Kommandos ab. Mit der im folgenden erläuterten Vorgehensweise kann die Anzahl der Aufrufe des Kommandos auf einige wenige begrenzt werden, so dass der geschilderte Angriff auch bei einem relativ schwachen Verschlüsselungsverfahren und einem kurzen Schlüssel nahezu aussichtslos ist.

Der Durchlauf des Flußdiagramms beginnt mit einem Schritt S1, der bei einem Aufruf des Befehls INTERNAL AUTHENTICATE als erstes ausgeführt wird und bei dem abgefragt wird, ob der Fehlbedienungszähler FBZ kleiner als ein vorgebbarer Schwellwert MAX ist. Falls diese Bedingung nicht erfüllt ist, ist der Durchlauf des Flußdiagramms beendet, d. h. es werden weder die beim Befehl INTERNAL AUTHENTICATE vorgesehene Verschlüsselung noch irgendwelche anderen Befehle des Flußdiagramms ausgeführt. Falls die Abfrage im Schritt S1 erfüllt ist, d. h. der Fehlbedienungszähler FBZ kleiner als der Schwellwert MAX ist, schließt sich an Schritt S1 ein Schritt S2 an, bei dem der Fehlbedienungszähler FBZ inkrementiert wird. Danach folgt ein Schritt S3, bei dem die eigentliche Abarbeitung des Kommandos INTERNAL AUTHENTICATE durchgeführt wird, d. h. insbesondere die Verschlüsselung erfolgt. Die Zugehörigkeit der Schritte S1, S2 und S3 zu dem Kommando INTERNAL AUTHENTICATE wird durch eine gestrichelt dargestellte Umrahmung veranschaulicht.

An Schritt S3 schließt sich ein Schritt S4 an, in dem ein mit INITIALISE bezeichnetes Kommando ausgeführt wird. Bei diesem Kommando werden Initialisierungen durchgeführt, wobei die Details hierzu für die Erfindung

nicht relevant sind. Auf Schritt S4 folgt mit einem Schritt S5 die Ausführung eines Kommandos PURCHASE, bei dem mit dem Datenträger ein Zahlungsvorgang innerhalb einer Börsenanwendung durchgeführt wird. Wie durch eine gestrichelte Umrahmung angedeutet ist, schließt die Ausführung des Kommandos PURCHASE auch einen Schritt S6 und einen Schritt S7 mit ein. Im Schritt S6, der unmittelbar auf Schritt S5 folgt, wird abgefragt , ob die Durchführung des Kommandos PURCHASE gemäß Schritt S5 erfolgreich verlaufen ist. Falls dies der Fall ist, wird als nächstes der Schritt S7 ausgeführt, bei dem der Fehlbedienungszähler FBZ zurückgesetzt wird. Mit der Ausführung des Schrittes S7 ist der Durchlauf des Flußdiagramms beendet. Ist die Abfrage des Schrittes S6 nicht erfüllt, so wird der Durchlauf des Flußdiagramms ohne Rücksetzung des Fehlbedienungszählers FBZ beendet.

Insgesamt ergibt sich somit, dass eine Ausführung des Kommandos INTERNAL AUTHENTICATE nur dann möglich ist, wenn der Fehlbedienungszähler FBZ noch nicht den Schwellwert MAX erreicht hat und dass der Fehlbedienungszähler FBZ bei jeder Ausführung des Kommandos inkrementiert wird. Ein Rücksetzen des Fehlbedienungszählers FBZ erfolgt nur dann, wenn das Kommando PURCHASE gemäß Schritt S5 erfolgreich ausgeführt wurde, so dass ohne eine erfolgreiche Ausführung des Kommandos PURCHASE die Anzahl der Ausführungen des Kommandos INTERNAL AUTHENTICATE auf Werte unterhalb des Schwellwerts MAX begrenzt wird. Alternativ zur Darstellung der Fig. 1 ist es auch möglich, das Rücksetzen des Fehlbedienungszähler FBZ an eine erfolgreiche Ausführung des Kommandos INITIALISE zu knüpfen.

Fig. 2 zeigt ein Flußdiagramm für eine weitere Kommandosequenz, bei der wiederum das Kommando INTERNAL AUTHENTICATE abgesichert wird. Diese Kommandosequenz zeichnet sich dadurch aus, dass die Rücksetzung

des Fehlbedienungszählers FBZ im Rahmen einer PIN-Prüfung erfolgt, bei der ermittelt wird, ob eine Geheimzahl richtig eingegeben wurde. Die Ausführungen zu Fig. 1 gelten für diese Kommandosequenz entsprechend und auch der Verfahrensablauf ist analog ausgebildet. Die Schritte S8, S9 und S10 folgen in dieser Reihenfolge aufeinander und stimmen identisch mit dem Schritten S1, S2 und S3 der Fig. 1 überein. An Schritt S10 schließt sich ein Schritt S11 an, in dem die PIN-Prüfung durchgeführt wird. In einem darauffolgenden Schritt S12 wird abgefragt, ob die PIN-Prüfung erfolgreich verlief. Wenn dies der Fall ist, wird anschließend in einem Schritt S13 der Fehlbedienungszähler FBZ zurückgesetzt und der Durchlauf des Flußdiagramms ist beendet. Andernfalls wird der Durchlauf des Flußdiagramms ohne Zurücksetzen des Fehlbedingungszählers FBZ beendet. Bei diesem Ausführungsbeispiel ist die Zugehörigkeit der Schritte S8, S9 und S10 zum Kommando INTERNAL AUTHENTICATE sowie der Schritte S11, S12 und S13 zur PIN-Prüfung jeweils durch eine gestrichelte Umrahmung dargestellt.

Fig. 3 zeigt ein Flußdiagramm für eine nochmals andere Kommandosequenz, wobei ein Kommando GET CHALLENGE abgesichert wird. Bei diesem Kommando wird eine Zufallszahl von Datenträger beispielsweise mit einem Kryptoalgorithmus erzeugt. Durch die Anwendung des erfindungsgemäßen Verfahrens soll die Generierungsprozedur gegen beliebig viele Aufrufe geschützt werden. Auch für die Kommandosequenz der Fig. 3 haben die Ausführungen zu Fig. 1 in entsprechender Weise Gültigkeit. Gemäß dem Flußdiagramm der Fig. 3 wird zunächst ein Schritt S14 und dann ein Schritt S15 ausgeführt, die den Schritten S1 und S2 der Fig. 1 identisch entsprechen. Auf Schritt S15 folgt ein Schritt S16, der die eigentliche Durchführung des Kommandos GET CHALLENGE repräsentiert, d. h. die Erzeugung der Zufallszahl. Durch eine gestrichelte Umrahmung ist verdeutlicht, dass die Schritte S14, S15 und S16 dem Kommando GET CHALLENGE zuzuordnen sind. An

Schritt S16 schließt sich ein Schritt S17 an, in dem ein Kommando ausgeführt wird, für das sich durch den Datenträger nachprüfen lässt, ob die Ausführung autorisiert war. Um welches Kommando es sich dabei im einzelnen handelt, ist zweitrangig. Als nächstes wird in einem Schritt S18 geprüft, ob das Kommando erfolgreich ausgeführt wurde, d. h. ob die erforderliche Autorisierung vorlag. Die Autorisierung wird in der Regel anhand einer dem Datenträger übermittelten Information überprüft. Falls die Prüfung positiv verläuft, schließt sich ein Schritt S19 an, bei dem der Fehlbedienungszähler FBZ zurückgesetzt wird. Damit ist der Durchlauf des Flußdiagramms beendet. Ergibt die Prüfung in Schritt S18, dass das Kommando nicht erfolgreich durchgeführt wurde, wird der Durchlauf des Flußdiagramms ohne Rücksetzung des Fehlerzählers FBZ beendet.

Mit dem erfindungsgemäßen Verfahren lassen sich nicht nur die explizit genannten Kommandos gegen ein beliebiges Aufrufen absichern, sondern beispielsweise auch ein Kommando CALCULATE MAC, bei dem eine Prüfsumme berechnet wird oder ein Kommando SIGN, bei dem eine digitale Signatur erstellt wird usw. Das Prüfen und Inkrementieren des Fehlbedienungszählers FBZ findet dabei jeweils bevorzugt vor der eigentlichen Ausführung des Kommandos statt, um potentielle Manipulationen möglichst zu erschweren.

Seitens des Endgeräts sind für den Einsatz des erfindungsgemäßen Verfahrens keine Änderungen erforderlich, d. h. es können unverändert die üblichen Kommandos an den Datenträger übermittelt werden. Beim Einsatz des erfindungsgemäßen Verfahrens ändert sich lediglich die interne Abarbeitung der Kommandos im Datenträger.

Patentansprüche

1. Verfahren zum Schutz eines tragbaren Datenträgers, wobei ein Fehlbedienungszähler (FBZ) vorgesehen ist, mit dem die Anzahl der Aufrufe einer Aktion des Datenträgers erfasst wird und wobei eine Durchführung der Aktion nur dann zugelassen wird, wenn der Fehlbedienungszähler (FBZ) unterhalb eines vorgebbaren Schwellwerts (MAX) liegt, dadurch **gekennzeichnet**, dass der Fehlbedienungszähler (FBZ) mehreren Aktionen des Datenträgers zugeordnet wird, indem ein Inkrementieren des Fehlbedienungszählers (FBZ) bei einem Aufruf einer ersten Aktion und ein Rücksetzen des Fehlbedienungszählers (FBZ) bei einer erfolgreichen Durchführung einer zweiten Aktion erfolgt.

2. Verfahren nach Anspruch 1, dadurch **gekennzeichnet**, dass die erste Aktion und die zweite Aktion in eine Sequenz eingebunden sind, so dass bei einem ordnungsgemäßen Betrieb des Datenträgers bei einer Ausführung der ersten Aktion stets auch die zweite Aktion ausgeführt wird.

3. Verfahren nach einem der vorhergehenden Ansprüche, dadurch **gekennzeichnet**, dass zwischen der ersten und der zweiten Aktion wenigstens eine weitere Aktion ausgeführt wird.

4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch **gekennzeichnet**, dass zu Beginn der ersten Aktion überprüft wird, ob der Fehlbedienungszähler (FBZ) unterhalb des Schwellwerts (MAX) liegt und eine Durchführung der ersten Aktion nur dann zugelassen wird, wenn die Überprüfung ein positives Ergebnis liefert.

5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch **gekennzeichnet**, dass der Fehlbedienungszähler (FBZ) zu Beginn der ersten Aktion inkrementiert wird.

6. Verfahren nach einem der vorhergehenden Ansprüche, dadurch **gekennzeichnet**, dass bei der Durchführung der ersten Aktion geheime Daten verarbeitet und/oder geheime Algorithmen angewendet werden.

7. Verfahren nach einem der vorhergehenden Ansprüche, dadurch **gekennzeichnet**, dass die erste Aktion in einer Erzeugung einer Zufallszahl, einer Verschlüsselung einer Zeichenfolge, einer Berechnung einer Prüfsumme oder einer Erzeugung einer digitalen Signatur besteht.

8. Verfahren nach einem der vorhergehenden Ansprüche, dadurch **gekennzeichnet**, dass bei der Durchführung der ersten Aktion vom Datenträger nicht geprüft wird, ob eine autorisierte Benutzung des Datenträgers vorliegt.

9. Verfahren nach einem der vorhergehenden Ansprüche, dadurch **gekennzeichnet**, dass bei der Durchführung der zweiten Aktion eine dem Datenträger übermittelte Information geprüft wird und der Fehlbedienungszähler (FBZ) zurückgesetzt wird, wenn die Prüfung erfolgreich verläuft.

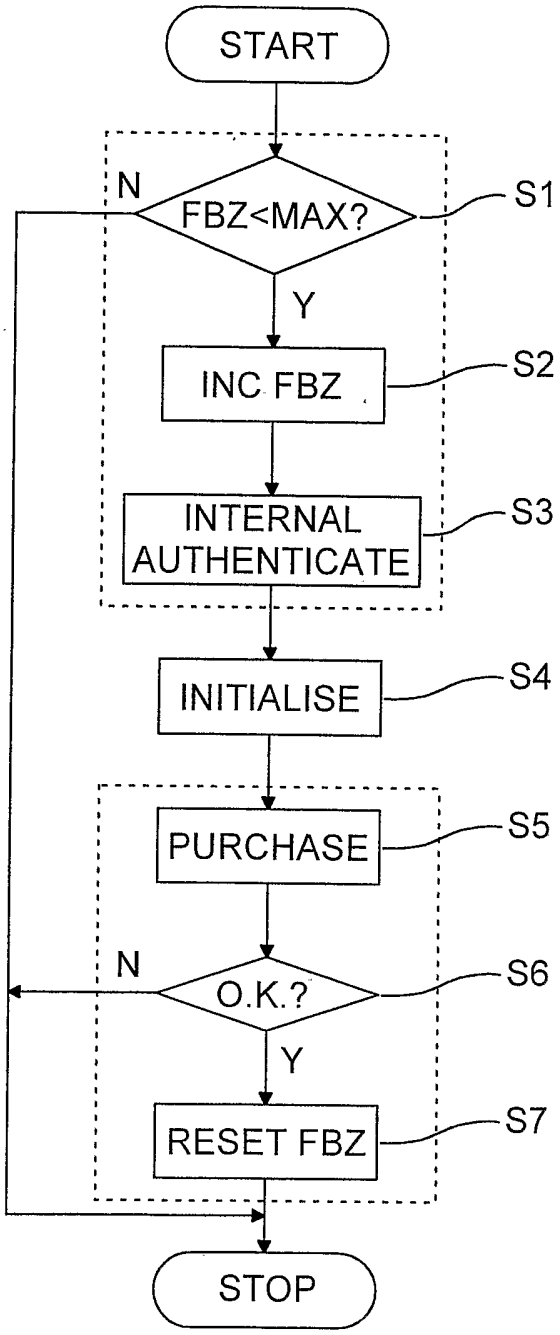

START
N
FBZ<MAX?
S1
Y
INC FBZ
S2
INTERNAL AUTHENTICATE
S3
INITIALISE
S4
PURCHASE
S5
N
O.K.?
S6
Y
RESET FBZ
S7
STOP

Fig. 1

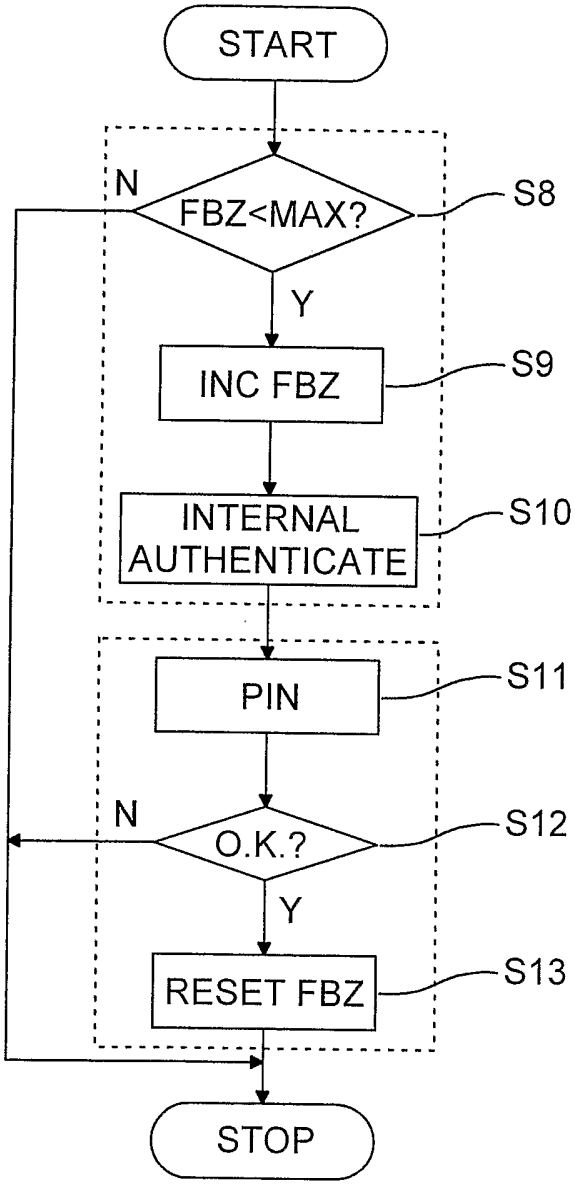

START
N
FBZ<MAX?
S8
Y
INC FBZ
S9
INTERNAL AUTHENTICATE
S10
PIN
S11
N
O.K.?
S12
Y
RESET FBZ
S13
STOP

Fig. 2

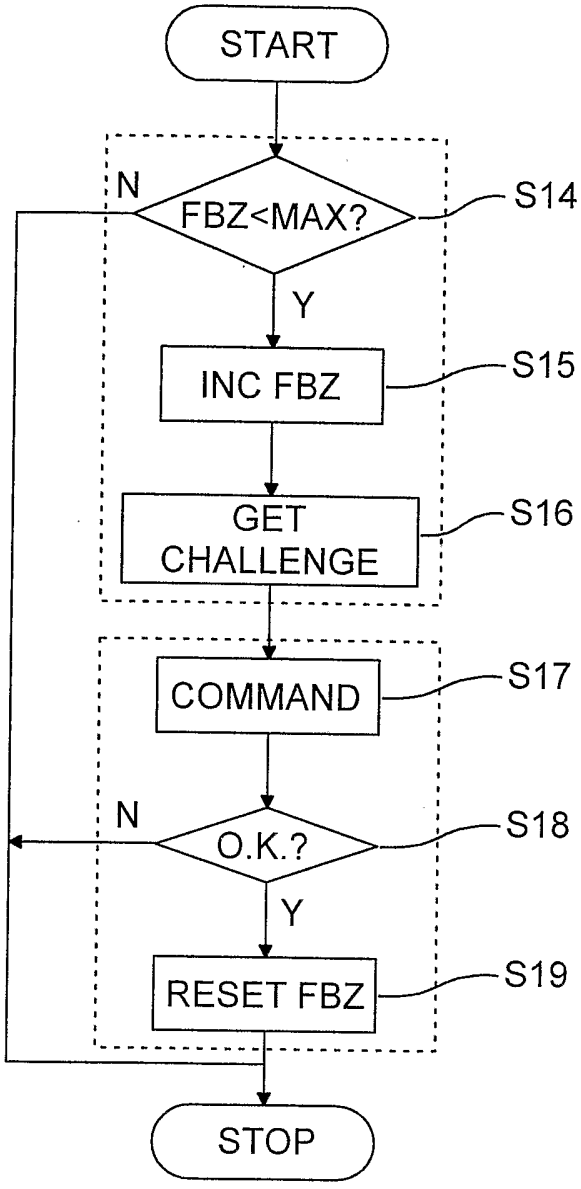

START
N
FBZ<MAX?
S14
Y
INC FBZ
S15
GET
CHALLENGE
S16
COMMAND
S17
N
O.K.?
S18
Y
RESET FBZ
S19
STOP

Fig. 3

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 03/12249

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DE 43 39 460 C (SIEMENS AG) 6 April 1995 (1995-04-06) cited in the application column 3, line 40 -column 4, line 27 figure 1	1-19
X	EP 0 570 924 A (SIEMENS AG) 24 November 1993 (1993-11-24) figure 1	1-19
A	EP 0 973 134 A (IBM) 19 January 2000 (2000-01-19) the whole document	1-19
A	WO 00/30049 A (VALADIER JEAN LOUIS ;GEMPLUS CARD INT (FR)) 25 May 2000 (2000-05-25) the whole document	1-19

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

'A' document defining the general state of the art which is not considered to be of particular relevance

'E' earlier document but published on or after the international filing date

'L' document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

'O' document referring to an oral disclosure, use, exhibition or other means

'P' document published prior to the international filing date but later than the priority date claimed

'T' later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

'X' document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

'Y' document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

'&' document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
8 April 2004	03/05/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Fleckinger, C

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP 03/12249

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
DE 4339460	C	06-04-1995	DE	4339460 C1	06-04-1995
			EP	0654919 A2	24-05-1995
EP 0570924	A	24-11-1993	DE	59308837 D1	10-09-1998
			DK	570828 T3	10-05-1999
			EP	0570828 A2	24-11-1993
			EP	0570924 A2	24-11-1993
			ES	2119832 T3	16-10-1998
EP 0973134	A	19-01-2000	DE	19831884 A1	20-01-2000
			CN	1245311 A	23-02-2000
			DE	69909379 D1	14-08-2003
			EP	0973134 A1	19-01-2000
			JP	2000047945 A	18-02-2000
			KR	2000011286 A	25-02-2000
			TW	528959 B	21-04-2003
			US	6711685 B1	23-03-2004
WO 0030049	A	25-05-2000	FR	2786007 A1	19-05-2000
			AU	1167200 A	05-06-2000
			CN	1333904 T	30-01-2002
			EP	1131800 A1	12-09-2001
			WO	0030049 A1	25-05-2000

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 03/12249

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G06F1/00 G07F7/10

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G06F G07F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	DE 43 39 460 C (SIEMENS AG) 6. April 1995 (1995-04-06) in der Anmeldung erwähnt Spalte 3, Zeile 40 -Spalte 4, Zeile 27 Abbildung 1	1-19
X	EP 0 570 924 A (SIEMENS AG) 24. November 1993 (1993-11-24) Abbildung 1	1-19
A	EP 0 973 134 A (IBM) 19. Januar 2000 (2000-01-19) das ganze Dokument	1-19
A	WO 00/30049 A (VALADIER JEAN LOUIS ;GEMPLUS CARD INT (FR)) 25. Mai 2000 (2000-05-25) das ganze Dokument	1-19

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
8. April 2004	03/05/2004

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Fleckinger, C

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP 03/12249

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
DE 4339460	C	06-04-1995	DE	4339460 C1	06-04-1995
			EP	0654919 A2	24-05-1995
EP 0570924	A	24-11-1993	DE	59308837 D1	10-09-1998
			DK	570828 T3	10-05-1999
			EP	0570828 A2	24-11-1993
			EP	0570924 A2	24-11-1993
			ES	2119832 T3	16-10-1998
EP 0973134	A	19-01-2000	DE	19831884 A1	20-01-2000
			CN	1245311 A	23-02-2000
			DE	69909379 D1	14-08-2003
			EP	0973134 A1	19-01-2000
			JP	2000047945 A	18-02-2000
			KR	2000011286 A	25-02-2000
			TW	528959 B	21-04-2003
			US	6711685 B1	23-03-2004
WO 0030049	A	25-05-2000	FR	2786007 A1	19-05-2000
			AU	1167200 A	05-06-2000
			CN	1333904 T	30-01-2002
			EP	1131800 A1	12-09-2001
			WO	0030049 A1	25-05-2000