(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
26. Februar 2009 (26.02.2009)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2009/024326 A2

(51) Internationale Patentklassifikation:
G06K 19/073 (2006.01) *G06K 19/07* (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2008/006812

(22) Internationales Anmeldedatum:
19. August 2008 (19.08.2008)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2007 039 226.7 20. August 2007 (20.08.2007) 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)*: **URHAHN, Thorsten** [DE/DE]; Beimerstetter Strasse 5/1, 89081 Ulm (DE). **GREBE, Alexander** [DE/DE]; Am Oberfeld 6, 84405 Dorfen (DE).

(74) Anwalt: **KLUNKER.SCHMITT-NILSON.HIRSCH**; Destouchesstrasse 68, 80796 München (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Erklärungen gemäß Regel 4.17:
— *hinsichtlich der Berechtigung des Anmelders, ein Patent zu beantragen und zu erhalten (Regel 4.17 Ziffer ii)*
— *hinsichtlich der Berechtigung des Anmelders, die Priorität einer früheren Anmeldung zu beanspruchen (Regel 4.17 Ziffer iii)*
— *Erfindererklärung (Regel 4.17 Ziffer iv)*

Veröffentlicht:
— *ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts*

(54) **Title:** REAL TIME MEASUREMENT ON A PORTABLE DATA CARRIER

(54) **Bezeichnung:** ECHTZEITMESSUNG AUF EINEM PORTABLEN DATENTRÄGER

(57) **Abstract:** The invention relates to a portable data carrier (1) comprising at least one storage (4), one processor (2) for executing a program routine (8) present on the data carrier (1) as a real time constant process (9) and one communication unit (12) for data communication with an external communication device (25) via a communication interface (6) of the data carrier (1). The program routine (8) is designed in a way, such as to be carried out as real time constant process (9) by the processor (2) in an essentially constant execution time (t). A real time control (10) of the data carrier (1) effects the execution of the program routine (8) as real time process (9) by the processor (2) and determines a real time frame as a multiple of the execution time (t) of the real time constant process (9).

(57) **Zusammenfassung:** Ein erfindungsgemäßer portabler Datenträger (1) umfasst zumindest einen Speicher (4), einen Prozessor (2) zum Ausführen einer auf dem Datenträger (1) vorliegenden Programmroutine (8) als echtzeitkonstanten Prozess (9) und eine Kommunikationseinrichtung (12) zur Datenkommunikation mit einer externen Kommunikationsvorrichtung (25) über eine Kommunikationsschnittstelle (6) des Datenträgers (1). Die Programmroutine (8) ist ausgestaltet, von dem Prozessor (2) als echtzeitkonstanter Prozess (9) mit einer im Wesentlichen konstanten Ausführungsdauer (*t*) ausgeführt zu werden. Eine Echtzeitsteuerung (10) des Datenträgers (1) bewirkt die Ausführung der Programmroutine (8) als echtzeitkonstanten Prozess (9) durch den Prozessor (2) und bestimmt eine Echtzeitspanne als Vielfaches der Ausführungsdauer (*t*) des echtzeitkonstanten Prozesses (9).

WO 2009/024326 A2

Echtzeitmessung auf einem portablen Datenträger

Die vorliegende Erfindung betrifft ein Verfahren zum Bestimmen einer Echtzeitspanne in einem portablen Datenträger sowie einen derartigen portablen Datenträger.

Zumeist verwenden Chipkarten und ähnliche portable Datenträger als interne Zeitbasis ein generiertes Taktsignal, das nicht auf die natürliche Echtzeit abgestimmt ist. Hinzukommt, dass ein extern an der Chipkarte anliegender Takt von dem jeweiligen Taktgeber abhängig ist und verschieden sein kann. Ein derartiger portabler Datenträger hat also in der Regel keine Möglichkeit, die natürliche Echtzeit als Zeitpunkt oder Zeitspanne genau zu bestimmen, so dass eine echtzeitabhängige Steuerung des Datenträgers nicht möglich ist.

In diesem Zusammenhang ist es bekannt, eine Chipkarte mit einer separaten Zeitmesseinrichtung auszustatten, die eine Echtzeitbasis bereitstellt. Beispielsweise sehen die WO 01/54057 A1 und die US 2006/0163369 A1 jeweils eine separate Zeitmesseinheit vor, die unabhängig von äußeren Einflüssen sind, wie z.B. einem Taktsignal. Auch nach Wegfall der Energieversorgung der Chipkarte können diese Zeitmesseinrichtungen durch eine separate interne Energieversorgung zumindest zeitweise weiterbetrieben werden. Die Zeitmesseinrichtung der US 2006/0163369 A1 ermöglicht dabei, das Ablaufen einer vorgegebenen Echtzeitspanne zu erkennen oder eine bestimmte Operation innerhalb der Echtzeitspanne auszuführen. Die Zeitmesseinrichtung ist als kapazitive Komponente ausgestaltet, deren fortschreitende Entladung als Echtzeitbasis ver-

wendet wird. Derartige spezielle konstruktive Lösungen mit separaten (Hardware-) Echtzeitsteuerungen sind jedoch baulich aufwändig und entsprechend teuer.

Im Zusammenhang mit der Durchführung interaktiver TV/Computer-Spiele schlägt die US 5,850,447 vor, Benutzerstationen (Spielkonsolen) mit Zähleinrichtungen auszustatten, die eine Taktinformation erzeugen, um zentral ermitteln zu können, ob eine Benutzeraktion vor Ablauf einer bestimmten Zeitfrist stattgefunden hat. Hierbei ist jedoch die Bestimmung einer Echtzeitspanne nicht erforderlich, da lediglich eine chronologische Abfolge der Benutzeraktionen bestimmt wird.

Die DE 100 57 477 A1, die WO 01/61639 A1 sowie die EP 0 337 684 A2 betreffen jeweils die Bereitstellung eines internen Takts auf einer Chipkarte, unabhängig von einem extern anliegende Taktsignal und die Umschaltung zwischen einem externen und dem internen Takt. Eine interne Echtzeitbasis betreffen diese Schriften nicht.

Ferner offenbart die US 6,202,927 ein System zur Prozessüberwachung bei Chipkarten, dessen Sensoren Zeitinformationen bezüglich der überwachten Chipkartenprozesse liefern. Die EP 1 112 627 B1 offenbart ein Verfahren zum Verbreiten einer Zeitinformation in einem Funkkommunikationssystem, bei dem unterschiedliche Zeitbasen von Mobilfunkbasisstationen bestimmt werden. Die US 5,414,835 schlägt vor, dass ein Schreib-/Lesegerät im Rahmen des ATR-Signals („Answer-to-Reset") eine Zeitinformation an eine Chipkarte schickt, bis zu deren Ablauf das Schreib-/Lesegerät auf eine Antwort der Chipkarte wartet. Schließlich offenbart die EP 0 849 651 A1 ein Verfahren zum Synchronisieren eines internen Zeitgebers eines Funkempfängers durch ein Zeitinformationssignal einer Basisstation.

Demzufolge ist es die Aufgabe der vorliegenden Erfindung, auf einem portablen Datenträger eine Möglichkeit zum Ermitteln von Echtzeitspannen unabhängig von einem intern erzeugten oder extern angelegten Taktsignal bereitzustellen.

Diese Aufgabe wird erfindungsgemäß durch ein Verfahren sowie einen portablen Datenträger mit den Merkmalen der unabhängigen Ansprüche gelöst. In davon abhängigen Ansprüchen sind vorteilhafte Ausgestaltungen und Weiterbildungen der Erfindung angegeben.

Eine Echtzeitspanne wird in einem portablen Datenträger als Vielfaches einer im Wesentlichen konstanten Ausführungsdauer eines auf dem Datenträger aufgeführten echtzeitkonstanten Prozesses bestimmt. Dazu führt ein portabler Datenträger mit einem Prozessor zum Ausführen von in einem Speicher des Datenträgers vorliegenden Programmroutinen eine ausgewählte Programmroutine aus, deren besondere Eigenschaft es ist, als echtzeitkonstanter Prozess mit einer im Wesentlichen konstanten Ausführungsdauer ausführbar zu sein; d.h., die Ausführung der Programmroutine ist unabhängig von einem internen Takt des Prozessors oder einem extern an den Datenträger angelegten Taktsignal und erfordert eine im Wesentlichen unveränderliche Ausführungsdauer. Diese konstante Ausführungsdauer der ausgewählten Programmroutine repräsentiert die kleinste für den Datenträger messbare Zeiteinheit und kann mit jeder beliebigen anderen Zeiteinheit in Beziehung gesetzt werden, insbesondere auch mit dem üblichen Zeiteinheitsystem aus Sekunden, Minuten, Stunden, etc.

Zum Bestimmen einer Echtzeitspanne basierend auf der konstanten Ausführungsdauer der ausgewählten Programmroutine umfasst der Datenträger eine Echtzeitsteuerung, die die Echtzeitspanne als Vielfaches der konstanten Aus-

führungsdauer des entsprechenden echtzeitkonstanten Prozesses bestimmt, indem die Programmroutine so oft sequentiell wiederholend als echtzeitkonstanter Prozess ausgeführt wird, bis die zu bestimmende Echtzeitspanne abgemessen ist.

Als Programmroutine mit im Wesentlichen konstanter Ausführungsdauer werden solche Programmroutinen bevorzugt, die nicht auf einen Speicher des Datenträgers zugreifen, da Speicherzugriffe zumeist eine Koordination durch eine Speicherverwaltung erfordern, die nicht der Kontrolle des entsprechenden Prozesses unterliegt. Besonders geeignet als Programmroutine, die auf dem Datenträger als echtzeitkonstanter Prozess ausgeführt werden kann, ist die Erzeugung von Zufallszahlen, so dass die einmalige Erzeugung einer Zufallszahl die echtzeitkonstante Zeitbasis des Datenträgers bildet. Diese interne Zeitbasis kann dann mit der Echtzeit in Bezug gesetzt werden, indem die Echtzeitsteuerung die Programmroutine fortlaufend sequentiell als kontinuierliche Wiederholung entsprechender echtzeitkonstanter Prozesse ausführt und dadurch ermöglicht, eine bestimmte Echtzeitspanne über die Anzahl der Ausführungen des echtzeitkonstanten Prozesses und deren konstanter Ausführungszeit in Bezug zu setzen.

Die fortlaufende, sequentiell wiederholte Ausführung der Programmroutine wird dadurch realisiert, dass nach der Abarbeitung eines echtzeitkonstanten Prozesses der nächste echtzeitkonstante Prozess möglichst unmittelbar im Anschluss daran gestartet wird, so dass eine vernachlässigbare zeitliche Lücke zwischen der Beendigung eines echtzeitkonstanten Prozesses und dem Beginn des darauf folgenden echtzeitkonstanten Prozesses entsteht.

Die Echtzeitsteuerung kann die fortlaufend sequentiell wiederholte Ausführung der Programmroutine als echtzeitkonstanten Prozess zu jedem beliebigen

Zeitpunkt starten, z.B. unmittelbar bei der Inbetriebnahme des Datenträgers oder bei einem bestimmten datenträgerinternen Ereignis, von dem ausgehend eine Echtzeitspanne zu bestimmen ist. Hierzu kann der Datenträger eine Überwachungseinrichtung umfassen, die ein Eintreten eines solchen vorgegebenen Ereignisses oder eines vorgegebenen internen Zustandes des Datenträgers erkennt und ein entsprechendes Auslösesignal an die Echtzeitsteuerung sendet, wobei diese bei Empfang des Auslösesignals die fortlaufend sequentiell wiederholte Ausführung der Programmroutine durch entsprechend zeitlich abgestimmte Programmaufrufe der Programmroutine bewirkt.

Falls nur eine relativ ungenaue Echtzeitmessung erforderlich ist, ist es ausreichend, die Ausführung der Programmroutine nur dann fortlaufend sequentiell zu wiederholen, wenn der Prozessor keinen von dem speziellen echtzeitkonstanten Prozesse verschiedenen Prozess ausführt bzw. nur eine geringe Auslastung aufweist, also möglichst während der „Idle-Zeiten" des Prozessors. Eine Überwachungseinrichtung des Datenträgers kann, wenn ein solcher Zustand eintritt, ein Auslösesignal an die Echtzeitsteuerung senden. Entsprechend sendet die Überwachungseinrichtung ein Beendigungssignal an die Echtzeitsteuerung, sobald die Auslastung des Prozessor signifikant ansteigt, z.B. weil ein von dem echtzeitkonstanten Prozess verschiedener Prozess ausgeführt wird. Die fortlaufend sequentiell wiederholte Ausführung der Programmroutine als echtzeitkonstanter Prozess wird dann nur zwischen dem Empfang des Auslösesignals und des Beendigungssignals durchgeführt.

Bei einer Chipkarte wird die fortlaufend sequentiell wiederholte Ausführung der Programmroutine vorzugsweise dann durchgeführt, wenn die Chipkarte eine Antwortnachricht (R-APDU; „Response Application Protocol Data Unit") an eine externe Kommunikationseinrichtung, z.B. ein Schreib-/Lesegerät geschickt hat, und auf die nächste Anfragenachricht (C-APDU; „Command Appli-

cation Protocol Data Unit") der Kommunikationsvorrichtung wartet, also zwischen einer Beantwortung einer Anfrage durch die Chipkarte und der nächsten Anfrage der externen Kommunikationsvorrichtung. Die Kommunikation des Datenträgers mit einer externen Kommunikationsvorrichtung wird dabei vorzugsweise von einer Kommunikationseinrichtung des Datenträgers durchgeführt, die eine Kommunikationsverbindung zu der externen Kommunikationsvorrichtung aufbaut und eine Datenkommunikation über eine entsprechende Kommunikationsschnittstelle des Datenträgers mit der externen Kommunikationsvorrichtung durchführt. Die Überwachungseinrichtung steht mit der Kommunikationseinrichtung in Kontakt, um das Senden einer Antwortnachricht bzw. das Empfangen einer Anfragenachricht ausreichend zu erkennen.

Falls die Überwachungseinrichtung das Eintreten eines vorgegebenen Ereignisses auf dem Datenträger der Echtzeitsteuerung durch ein Auslösesignal mitteilt, kann die Echtzeitsteuerung eine bestimmte Echtzeitzeitspanne ab Eintreten des Ereignisses mithilfe der fortlaufend sequentiellen Ausführung der ausgewählten Programmroutine abmessen und anschließend über die Ausführungsdauer des entsprechenden echtzeitkonstanten Prozesses den Ablauf dieser Echtzeitspanne erkennen.

Bei einer bevorzugten Ausführungsform wird die Beendigung der Ausführung eines einzelnen echtzeitkonstanten Prozesses durch eine Unterbrechung („Interrupt") - vorzugsweise durch eine Hardware-Unterbrechung - ausgelöst, woraufhin die zugehörige Unterbrechungsroutine (ISR; „Interrupt Service Routine") den Zählerstand eines in einem Speicher des Datenträgers eingerichteten Zeitzählers inkrementiert. Danach wird die fortlaufend sequentielle Ausführung des echtzeitkonstanten Prozesses mit dem erneuten Aufruf der Programmroutine fortgesetzt. Der Zeitzähler protokolliert somit die Anzahl der Ausführungen der Programmroutine als echtzeitkonstanten Prozess. Aus dem

aktuellen Zählerstand des Zeitzählers kann die Echtzeitsteuerung die verstrichene Zeit bestimmen, indem der aktuelle Zählerstand des Zeitzählers ausgelesen und mit der konstanten Ausführungsdauer des echtzeitkonstanten Prozesses multipliziert wird.

Auf diese Weise kann in einem Speicher des Datenträgers ein Betriebszeitzähler eingerichtet werden, dessen Zählerstand die Anzahl der fortlaufend sequentiell wiederholten Ausführungen der Programmroutine seit der letzten Inbetriebnahme des Datenträgers wiedergibt, sofern die Echtzeitsteuerung die fortlaufend sequentielle Ausführung der Programmroutine beginnt, sobald an dem Datenträger eine Versorgungsspannung anliegt. Das Inkrementieren eines derartigen Betriebszeitzählers kann hierbei wieder durch eine (Hardware-) Unterbrechung eingeleitet werden. In jedem Falle kann ein Datenträger eine Echtzeitspanne mittels der Echtzeitsteuerung nur messen, wenn er eine Versorgungsspannung (Vcc) und ein Taktsignal (CLK) von einer externen Kommunikationsvorrichtung, z.B. einem Schreib-/Lesegerät, empfängt.

Prinzipiell können in einem Speicher des Datenträgers beliebig viele verschiedene Zeitzähler unabhängig voneinander angelegt werden, die zur Bestimmung einer Vielzahl von unterschiedlichen Echtzeitspannen, z.B. ausgehend von unterschiedlichen datenträgerinternen Ereignissen, z.B. verschiedenen Softwarelizenzen oder Zugangsberechtigungen, verwendet werden. Die fortlaufend sequentielle Ausführung des echtzeitkonstanten Prozesses wir dabei vorzugsweise in einer einzigen Programmschleife durchgeführt, die die Zeitbasis für alle Zähler bildet, wobei die verschiedenen Zähler unabhängig voneinander durch entsprechende Unterbrechungsroutinen inkrementiert werden.

Einer dieser unabhängigen Zeitzähler, insbesondere der Betriebszeitzähler, kann als Referenzzeitzähler des Datenträgers eingesetzt werden, von dem wei-

tere Zeitzähler abgeleitet werden können, indem ein Zählerstand eines abgeleiteten Zeitzählers auf dem jeweiligen aktuellen Zählerstand des Referenz- oder Betriebszeitzählers basiert. Dies kann derart durchgeführt werden, dass ein abgeleiteter Zeitzähler um die Differenz der Zählerstände des Betriebszeitzählers zwischen zwei Aktualisierungszeitpunkten inkrementiert wird.

Zur Inkrementierung des Zählerstands des Betriebszeitzählers wird vorzugsweise nach jeder einzelnen Ausführung des echtzeitkonstanten Prozesses eine Unterbrechung ausgelöst, so dass die zugehörige Unterbrechungsroutine den Zählerstand des Betriebszeitzählers inkrementiert. Auch zur Aktualisierung des Zählerstandes eines abgeleiteten Zeitzählers wird vorzugsweise eine Unterbrechung ausgelöst, wobei die entsprechende Unterbrechungsroutine den Zählerstand des betreffenden abgeleiteten Zeitzählers basierend auf dem aktuellen Zählerstand des Betriebszeitzählers bzw. basierend auf dessen Differenz zu dem Zählerstand des Betriebszeitzählers bei der letzten Aktualisierung aktualisiert. Hierbei ist der Datenträger vorzugsweise derart eingerichtet, dass die Unterbrechungen auch in einem stromsparenden Modus des Datenträgers ausgelöst werden.

In einer besonders bevorzugten Ausführungsform wird ein Datenträger bereitgestellt, der eine Echtzeitspanne in einer unmanipulierbaren Art und Weise bestimmt, so dass insbesondere die Betriebszeit („Power-up-Zeit") des Datenträgers nicht von außen manipuliert werden kann. Dazu wird der portable Datenträger als Sicherheitsdatenträger, insbesondere als „Security IC" (SIC) oder Smart Card ausgestaltet, der z.B. besonders gesicherte Kommunikationsverbindungen zu einer externen Kommunikationsvorrichtung unterstützt. Die Zeitzähler, insbesondere der Betriebszeitzähler, werden in einem nicht-volatilen Speicher als persistente Zähler bzw. Datenstrukturobjekte eingerichtet, die gesondert gegen ein Auslesen von außen gesichert werden können.

Es ist auch möglich, dass der Betriebszeitzähler mittels eines externes Zeitsynchronisationssignals synchronisiert wird, das die Echtzeitsteuerung über die Kommunikationsschnittstelle von einer externen Kommunikationsvorrichtung empfängt. Sofern dieses Zeitsynchronisationssignal eine Echtzeit umfasst, kann diese von der Echtzeitsteuerung in die Zeitbasis des Datenträgers, d.h. die Ausführungsdauer des echtzeitkonstanten Prozesses, umgerechnet werden und zur Aktualisierung und Synchronisierung der Zeitzähler dienen. Bei regelmäßigem Empfang eines Synchronisationssignals (z.B. einige Minuten oder jede Stunde) kann das Zeitintervall zwischen zwei Synchronisationssignalen in die Zeitbasis des Datenträgers, d.h. in die Ausführungsdauer des echtzeitkonstanten Prozesses, umgerechnet werden und zur etwaigen Korrektur der Betriebszeitzählers verwendet werden. Durch die Synchronisierung wird die Genauigkeit der internen Zeitmessung verbessert.

Die Echtzeitsteuerung kann ferner dazu eingerichtet sein, die Zählerstände der Zeitzähler, insbesondere des Betriebszeitzählers, durch die Überwachungseinrichtung auf Überschreiten eines vorgegebenen Zählerstands überwachen zu lassen, und bei Vorliegen einer Zählerstandüberschreitung über die Kommunikationseinrichtung des Datenträgers ein entsprechendes Benachrichtigungssignal an eine externe Kommunikationsvorrichtung zu senden. Dies kann beispielsweise den Ablauf einer Lizenzdauer oder einer Zugangsberechtigung betreffen. Der Datenträger gibt dadurch lediglich preis, dass ein vorgegebener Zählerstand erreicht und insofern eine vorgegebene Echtzeitspanne überschritten wurde. In ähnlicher Weise kann die Echtzeitsteuerung mittels der Kommunikationseinrichtung die vollständige Betriebszeit des Datenträgers basierend auf dem aktuellen Zählerstand des Betriebszeitzählers mittels eines Betriebszeitsignals an eine externe Kommunikationsvorrichtung senden.

Hierbei wird sämtliche Datenkommunikation des Datenträgers, die eine Echtzeitbestimmung oder Synchronisierung betrifft, vorzugsweise besonders abgesichert durchgeführt, indem die Kommunikationseinrichtung vor der Datenkommunikation eine sichere Kommunikationsverbindung zu der externen Kommunikationsvorrichtung aufbaut. Zusätzlich oder alternativ kann eine derartige Datenkommunikation mit einer externen Kommunikationsvorrichtung durch eine Verschlüsselung kryptographisch gesichert werden oder zumindest signiert werden, um den Datenträger gegenüber der externen Kommunikationsvorrichtung zu authentisieren.

Weitere Merkmale der Erfindung ergeben sich aus der folgenden Beschreibung verschiedener erfindungsgemäßer Ausführungsbeispiele und Ausführungsalternativen. Es wird auf die folgenden Figuren verwiesen, welche zeigen:

Fig. 1 eine schematische Übersicht des erfindungsgemäßen Verfahrens; und

Fig. 2 einen erfindungsgemäß eingerichteten portablen Datenträger zum Ausführen des Verfahrens nach Fig. 1.

Portable Datenträger, wie z.B. Chipkarten, Smart Cards, sichere Multimedia-Karten (MMC), Mobilfunkkarten oder dergleichen, benötigen für viele Anwendungen eine Echtzeitbasis, um Zeitspannen in der natürlichen Echtzeit in Millisekunden, Sekunden, Stunden etc. als so genannte Echtzeitspannen messen oder abgleichen zu können. Hierfür eignet sich weder ein internes Taktsignal noch ein von außerhalb des Datenträgers an diesen angelegtes externes Taktsignal, da einerseits die entsprechenden Taktraten variabel und abhängig von einem externen Schreib-/Lesegerät sein können, mit dem ein portabler Datenträger in Kontakt steht, und andererseits derartige Taktsignale nicht in jedem Fall in eine Echtzeit umzurechnen sind. Anwendungen, die die Bestimmung

einer Echtzeitspanne erfordern sind z.B. die Bestimmung der Betriebszeit des portablen Datenträgers, die Steuerung zeitabhängiger Lizenzen auf dem Datenträger oder auch die Echtzeiterfassung mittels des Datenträgers, z.B. um Arbeitszeiten oder Login-Zeiten eines Benutzers protokollieren zu können. Bei den meisten dieser Anwendungen ist es darüber hinaus notwendig, eine Manipulation von Echtzeitmessungen und deren Ergebnissen weitestgehend ausschließen zu können, weil mit den Zeitmessungen zumeist auch sicherheitsrelevante und/oder finanzielle Konsequenzen verbunden sind.

Die Grundlage einer derartigen Funktionalität eines portablen Datenträgers ist bei der in Fig. 2 gezeigten Chipkarte 1 die besonders ausgestaltete Programmroutine 8 (ROUT), die von einem Prozessor 2 (CPU) als echtzeitkonstanter Prozess 9 (RND) ausgeführt werden kann. Die Ausführung der Routine 8 als echtzeitkonstanter Prozess 9 ist unabhängig von einer internen und/oder externen Taktung der Chipkarte 1 bzw. des Prozessors 2 und benötigt eine Ausführungsdauer t, die hinreichend konstant ist, um als Echtzeitbasis der Chipkarte 1 zu dienen, d.h. als kleinste von der Chipkarte 1 ermittelbare konstante Zeiteinheit. Da die Ausführungsdauer t des echtzeitkonstanten Prozesses 9 bekannt ist, kann durch eine fortlaufend sequentiell wiederholte Ausführung des echtzeitkonstanten Prozesses 9 eine längere Echtzeitspanne abgemessen werden.

Bei der vorliegenden Ausführungsform der Erfindung wird als erfindungsgemäße Programmroutine 8 die Zufallszahlengenerierung (RND) verwendet, die den Vorteil hat, dass sie auf den meisten portablen Datenträgern als Funktion ohnehin vorhanden ist und deshalb nicht separat implementiert werden muss. Es können aber auch beliebige andere Programmroutinen 8 als Echtzeitbasis verwendet werden, sofern sie als echtzeitkonstante Prozesse 9 ausführbar sind, wozu insbesondere notwendig ist, dass derartige Programmroutinen 8 keine

Schreibzugriffe auf einen Speicher 5 des Datenträgers 1 durchführen, die die Ausführungsdauer der betreffenden Programmroutine 8 verzögern können.

Die Chipkarte 1 umfasst neben dem Prozessor 2 eine Kommunikationseinrichtung 12 (COM) und eine Kommunikationsschnittstelle 6 zur Kommunikation mit einer externen Kommunikationsvorrichtung, z.B. einem Schreib-/Lesegerät 25 oder dergleichen, sowie eine Speicheranordnung, die zumindest einen permanenten ROM-Speicher 3 sowie einen nicht-flüchtigen Speicher umfasst, z.B. einen EEPROM-Speicher oder einen Flash-Speicher 4 (FLASH). Darüber besitzt die Chipkarte 1 auch einen flüchtigen (RAM-) Arbeitsspeicher (nicht dargestellt). Die grundlegenden Funktionen der Chipkarte 1 werden von einem Chipkartenbetriebssystem 7 (OS) bereitgestellt, das in der Regel im ROM-Speicher 3 abgelegt ist. Darüber hinaus befinden sich im Flash-Speicher 4 weitere Programmroutinen oder Applikationen 10, 11, 12, die bei Bedarf auf dem Prozessor 2 ausgeführt werden können, sowie vielfältige persistent zu speichernde Daten bzw. Datenstrukturen 13, 14, 15.

In dem Flash-Speicher 4 befinden sich insbesondere die als echtzeitkonstanter Prozess 9 ausführbare Programmroutine 8, sowie eine Echtzeitsteuerung 10 (TME), eine Überwachungseinrichtung 11 (MON) und eine Kommunikationseinrichtung 12 (COM), die alle als von dem Prozessor 2 ausführbare Applikationen vorliegen. Zwischen diesen Komponenten 10, 11, 12 findet eine vielfältige Kommunikation in Form von Programmaufrufen und Signalen statt, beispielsweise mittels des Auslösesignals 18 des Beendigungssignals 19 zwischen der Überwachungseinrichtung 11 und der Echtzeitsteuerung 10, der Antwortnachricht 20 und der Anfragenachricht 21 zwischen der Kommunikationseinrichtung 12 und dem externen Schreib-/Lesegerät 12, sowie dem Benachrichtigungssignal 22 und dem Synchronisationssignal 23 an das bzw. von dem Schreib-/Lesegerät 25.

In dem nicht-flüchtigen Flash-Speicher 4 der Chipkarte 1 ist ein besonders abgesicherter und manipulationsgeschützter Speicherbereich 5 eingerichtet, in welchem verschiedene Zeitzähler angelegt sind, die zur Echtzeitmessung basierend auf der Ausführung der Programmroutine 9 eingesetzt werden, z.B. ein Betriebszeitzähler 13 (PCNT), der ein Maß für die Gesamtbetriebszeit der Chipkarte 1 wiedergibt, ein oder mehrere Ereigniszeitzähler 14 (ECNT), die ein Maß für eine Zeitspanne seit dem Eintritt eines bestimmten internen Ereignisses der Chipkarte 1 wiedergeben, sowie mehrere abgeleitete Zeitzähler 15 (DCNT1, DTNC2), deren Zählerstände n' basierend auf den Zählerständen n, m des Betriebszeitzählers 13 oder eines Ereigniszeitzählers 14 ermittelt werden.

Das Betriebssystem 7 der Chipkarte 1 umfasst neben vielfältigen System- und Betriebsfunktionen auch eine oder mehrere Unterbrechungsroutinen 17 (ISR; „Interrupt Service Routine"), die bei Auftreten einer vorzugsweise Hardwaregesteuerten Unterbrechung 16 (IR), die einen aktuell von dem Prozessor 2 ausgeführten Prozess, z.B. den echtzeitkonstanten Prozess 9, unterbricht, eine prioritätshöhere zeitkritische Operation ausführt. Nach Ausführung der Unterbrechungsroutine 17 wird der unterbrochene Prozess fortgesetzt.

Die für die Zeitmessung maßgeblichen Funktionen der Chipkarte 1 werden von einem Sicherheitschip SIC („Security IC") bereitgestellt, der Teil der Chipkarte 1 ist oder diese bildet. Sämtliche mit der Echtzeitmessung im Zusammenhang stehende Kommunikation zwischen der Chipkarte 1 bzw. deren Kommunikationseinrichtung 12 und einem externen Schreib-/Lesegerät 25 ist darüber hinaus besonders gegen Manipulationen gesichert, beispielsweise durch Aufbauen eines sicheren Kommunikationskanals durch die Kommunikationseinrichtung 12 über die Kommunikationsschnittstelle 6 zu dem Schreib-/Lesegerät 25 oder indem die übertragenen Daten (Signale, Nachrichten, etc.) durch eine krypto-

graphische Einrichtung (nicht dargestellt) der Chipkarte 1 verschlüsselt oder zum Nachweis der Authentizität der Chipkarte 1 signiert werden.

Die nachfolgend beschriebene Echtzeitmessung kann die Chipkarte 1 mittels der Echtzeitsteuerung 10 und diversen Zeitzählern 13, 14, 15 nur dann vornehmen, wenn an der Chipkarte 1 sowohl eine Spannungsversorgung (Vcc) als auch ein Taktsignal (CLK) anliegt.

Die Funktionen und Interaktionen der geschilderten Komponenten und Einrichtungen einer derartigen Chipkarte 1 werden nachfolgend in Zusammenhang mit Figur 1 erläutert. Die Reihenfolge der angegebenen Schritte S1 bis S19 ist dabei nicht statisch zu verstehen, sondern kann sich je nach Betriebssituation ändern. Dabei können bestimmte Schritte insbesondere auch ganz entfallen oder (quasi-) parallel ausgeführt werden, sofern es die Abhängigkeiten der Schritte untereinander erlaubt.

Nach dem Einschalten (POWER UP) der Chipkarte 1 in Schritt S1, z.B. durch Bereitstellen einer Spannungsversorgung für die Chipkarte 1 durch ein externes Schreib-/Lesegerät 25, richtet die Echtzeitsteuerung 10 in Schritt S2 möglichst unmittelbar danach einen Betriebszeitzähler 13 (PCNT) ein. Das Einrichten des Betriebszeitzählers 13 umfasst die Initialisierung ($n = 0$) eines als Datenstruktur in dem Flash-Speicher 4 der Chipkarte 1 bereits vorhandenen Betriebszeitzählers 13. Sobald der Betriebszeitzähler 13 initialisiert ist, startet die Echtzeitsteuerung 10 die Programmroutine 8, die dann von dem Prozessor 2 als echtzeitkonstanter Prozess 8, z.B. zum Erzeugen einer einzelnen Zufallszahl (RND), in Schritt S3 einmalig ausgeführt wird. Nach der Ausführungszeit t eines echtzeitkonstanten Prozesses 9 (üblicherweise einige Millisekunden) wird die Programmroutine 8 in Schritt S4 unmittelbar anschließend jeweils erneut als echtzeitkonstanter Prozess 9 gestartet, so dass sich durch die fortlaufend sequentiell

wiederholte Ausführung der Programmroutine 8 durch die Echtzeitsteuerung 10 eine Endlosschleife in den Schritten S3, S4 ergibt, die vorzugsweise erst bei Ausschalten der Chipkarte 1, d.h. bei Abbrechen der Energieversorgung, beendet wird.

Aufgrund der fortlaufend sequentiellen Wiederholung des echtzeitkonstanten Prozesses 9 kann die Erzeugung einer Zufallszahl von der Chipkarte 1 als Zeitbasis verwendet werden, indem die Ausführungsdauer t als kleinste konstante Zeiteinheit mit der Echtzeit in Bezug gesetzt wird. Vorliegend erfordert die Erzeugung einer Zufallszahl durch den echtzeitkonstanten Prozess 9 z.B. $t = 4$ ms, so dass die Chipkarte 1 durch die Echtzeitsteuerung 10 Zeitspannen mit einer Genauigkeit von $t = 4$ ms messen kann. Demzufolge ist nach $n = 250$ fortlaufend sequentiellen Ausführungen des echtzeitkonstanten Prozesses 9 eine Sekunde vergangen.

Die Anzahl der Ausführungen des echtzeitkonstanten Prozesses 9 wird in dem eingangs initialisierten Betriebszeitzähler 13 protokolliert, indem die Beendigung jedes echtzeitkonstanten Prozesses 9 in Schritt S5 eine Unterbrechung 16 (IR) auslöst, woraufhin die zugehörige Unterbrechungsroutine 17 (ISR) den Betriebszeitzähler 13 in Schritt S6 inkrementiert ($n = n + 1$) und anschließend die Ausführung der Programmschleife S3, S4 fortsetzt. Die gesamte Betriebszeit der Chipkarte 1 wird dann von der Echtzeitsteuerung 10 als Produkt des Zählerstands n des Betriebszeitzählers 13 und der Echtzeitbasis t bestimmt ($n*t$). Die Betriebszeit $n*t$ wird von der Echtzeitsteuerung 10 in Schritt S7 mit einem Betriebszeitsignal 22 über die Kommunikationseinrichtung 12 an das externe Schreib-/Lesegerät 25 gesendet (UPTIME), entweder in regelmäßigen Abständen oder auf Anforderung einer externen Stelle.

Ferner ist auch möglich, den Betriebszeitzähler 13 oder jeden beliebigen anderen Zeitzähler 14, 15 in Schritt S8 von außen zu synchronisieren (SYNC), indem das Schreib-/Lesegerät 25 ein Synchronisationssignal 23 über die Kommunikationsschnittstelle 6 an die Echtzeitsteuerung 10 schickt. Das Synchronisationssignal 23 des Schreib-/Lesegeräts 25 kann beispielsweise auf einer externen Echtzeitquelle beruhen und regelmäßig, z.B. in Intervallen von einigen Minuten, an die Chipkarte 1 gesendet werden. Falls das Synchronisationssignal 23 z.B. in Abständen von fünf Minuten bei der Chipkarte 1 eingeht, kann die Echtzeitsteuerung 10 prüfen, ob der Vergleich des aktuellen Zählerstands des Betriebszeitzählers 13 und des Zählerstands beim letzten empfangenen Synchronisationssignal 23 einer Echtzeitspanne von fünf Minuten entspricht. Bei Bedarf kann der Zählerstand n korrigiert werden. Auf diese Weise lässt sich ein bestimmtes Maß an Genauigkeit der Zeitzähler 13, 14, 15 sicherstellen, selbst wenn die Ausführung der Schleife S3, S4 zeitliche Inkonstanzen aufweist, die möglicherweise aus einer Auslastung des Prozessors 2 resultieren.

Bei einigen Anwendungen wird eine lediglich ungenaue Zeitmessung benötigt. Dann kann es ausreichend sein, dass die Echtzeitsteuerung 10 die fortlaufend sequentielle Wiederholung des echtzeitkonsistenten Prozesses 9 in der Schleife S3, S4 nur während solcher Zeiten durchführt, in denen der Prozessor 2 keine signifikante Auslastung besitzt. Ein solcher Zustand liegt bei der Chipkarte 1 insbesondere bei der Wartezeit zwischen dem Senden einer Antwortnachricht 20 (Response-APDU) auf eine frühere Anfragenachricht des Schreib-/Lesegeräts 25 und dem Empfang der nächsten Anfragenachricht 21 (Command-APDU) des Schreib-/Lesegeräts 25 vor. Die fortlaufend sequentielle Wiederholung des echtzeitkonstanten Prozesses 9 wird also durch die Echtzeitsteuerung 10 nach Aussenden der Antwortnachricht 20 durch die Kommunikationseinrichtung 12 gestartet und nach Erhalt der darauf folgenden Anfragenachricht 21 wieder beendet. Eine derartige temporäre Ausführung des echt-

zeitkonstanten Prozesses 9 hat jedoch zur Folge, dass die Zeitmessung bei ansteigender Kommunikation zwischen der Chipkarte 1 und dem Schreib-/Lesegerät 25 entsprechend schlechter wird. Mit heuristischen Verfahren kann das Ergebnis einer solchen temporären, ungenauen Zeitmessung jedoch abhängig von einer geschätzten Auslastung des Prozessors auf die Gesamtbetriebszeit hochgerechnet werden. In diesem Zusammenhang ist es bei der in Fig. 2 gezeigten Chipkarte 1 vorteilhaft, dass der echtzeitkonstante Prozess 9 auch in einem stromsparenden Modus der Chipkarte 1 fortlaufend sequentiell wiederholt werden kann, da das Auslösen einer Unterbrechung 16 nach Beendigung eines einzelnen echtzeitkonstanten Prozesses 9 auch in dem stromsparenden Modus der Chipkarte 1 möglich ist.

Prinzipiell kann die Echtzeitsteuerung 10 basierend auf der durch die Programmschleife S3, S4 gegebene Echtzeitbasis eine beliebige Anzahl von parallelen oder abgeleiteten Zeitzählern 15 (DCNT*i*) einrichten, deren jeweilige Zählerstände n' unabhängig voneinander durch entsprechende Unterbrechungen 16 und Unterbrechungsroutinen 17 inkrementiert oder aktualisiert werden. In Schritt S9 wird ausgehend von dem Betriebszeitzähler 13 eine beliebige Anzahl von weiteren Zeitzählern 15 (DCNT*i*) abgeleitet (DERIVE), deren jeweilige Zählerstände n' nicht unmittelbar von der fortlaufend sequentiellen Ausführung des echtzeitkonstanten Prozesses 9 in der Schleife S3, S4 abhängen, sondern lediglich basierend auf einem aktuellen Zählerstand n des Betriebszeitzählers 13 bei Bedarf in Schritt S10 aktualisiert werden (UPDATE).

Diese Aktualisierung kann durch eine interne Aktualisierungsroutine (nicht dargestellt) des Datenträgers 1 z.B. bei Vorliegen einer bestimmten Aktualisierungsbedingung durchgeführt werden. So kann beispielsweise ein abgeleiteter Zähler 15 zur Arbeitszeitmessung bei Beginn der Arbeit eingerichtet und initialisiert werden und in regelmäßigen größeren Zeitintervallen, während einer

Arbeitspause oder bei Beendigung der Arbeit mit der Differenz der Zählerstände des Betriebszeitzählers 13 zu Beginn und zu Beendigung der Arbeit in Schritt S10 aktualisiert werden. Die Aktualisierung eines abgeleiteten Zeitzählers 15 braucht nicht durch Unterbrechungen angestoßen zu werden, da keine zeitkritische Operation hoher Priorität vorliegt.

Neben dem bei Einschalten der Chipkarte in Schritt S2 angelegten Betriebszeitzähler 13 kann die Echtzeitsteuerung 10 eine beliebige Anzahl von weiteren parallelen Zeitzählern 14, 15 einrichten. Z.B. kann ein Ereigniszeitzähler 14 (ECNT) in Schritt S11 in der Chipkarte 1 eingerichtet und in Schritt S12 initialisiert werden ($m = 0$). Der Ereigniszeitzähler wird beginnend mit dem Auftreten des betreffenden Ereignisses (EVNT) in Schritt S13, das durch die Überwachungseinrichtung 11 in Schritt S14 erkannt wird, sukzessive inkrementiert.

Nach Auftreten des Ereignisses in Schritt S13 kann der Ereigniszeitzähler 14 basierend auf der bereits für den Betriebszeitzähler 13 begonnenen fortlaufend sequentiellen Wiederholung des echtzeitkonstanten Prozesses 9 in den Schritten S3, S4 aktualisiert werden. Entsprechend wird der Ereigniszeitzähler 14 bei Beendigung jedes einzelnen echtzeitkonstanten Prozesses 9 nach Auftreten des Ereignisses durch eine Unterbrechung 16 in Schritt S15 und durch eine entsprechende Unterbrechungsroutine 17 in Schritt S16 ($m = m + 1$) aktualisiert.

Die Überwachungseinrichtung 11 der Chipkarte 1 kann sämtliche Zeitzähler 13, 14, 15 überwachen und bei Überschreiten ($n, n', m > s$) eines vorgegebenen Schwellenzählerstandes s eines der Zeitzähler 13, 14, 15 diesen in Schritt S18 als Benachrichtigungssignal 24 an die externe Schreib-/Leseeinrichtung 25 senden (REPORT) oder in Schritt S19 einen weiteren Prozess anstoßen, der in Reaktion auf den entsprechenden Zählerstand ausgeführt wird.

Patentansprüche

1. Verfahren zum Bestimmen einer Echtzeitspanne in einem portablen Datenträger (1), **dadurch gekennzeichnet**, dass die Echtzeitspanne als Vielfaches der im wesentlichen konstanten Ausführungsdauer (t) eines echtzeitkonstanten Prozesses (9) auf dem Datenträger (1) bestimmt wird.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet**, dass der echtzeitkonstante Prozess (9) nicht auf einen Speicher (4) des Datenträgers (1) zugreift.

3. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet**, dass als echtzeitkonstanter Prozess (9) ein Prozess zum Erzeugen zumindest einer Zufallszahl ausgeführt wird (S3).

4. Verfahren nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet**, dass eine Ausführung (S3) des echtzeitkonstanten Prozesses (9) fortlaufend sequentiell wiederholt wird (S4), solange auf dem Datenträger (1) kein von dem echtzeitkonstanten Prozess (9) verschiedener Prozess ausgeführt wird.

5. Verfahren nach Anspruch 4, **dadurch gekennzeichnet**, dass eine Ausführung (S3) des echtzeitkonstanten Prozesses (9) zwischen einem Senden einer Antwortnachricht (20) des Datenträgers (1) an eine externe Kommunikationseinrichtung (25) und einem Empfangen einer nächsten Anfragenachricht (21) durch den Datenträger (1) fortlaufend sequentiell wiederholt (S4) wird.

6. Verfahren nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet**, dass eine Ausführung (S3) des echtzeitkonstanten Prozesses (9) beginnend mit

einem Eintreten eines vorgegebenen Ereignisses (S13) auf dem Datenträger (1) fortlaufend sequentiell wiederholt (S4) wird.

7. Verfahren nach einem der Ansprüche 4 bis 6, **dadurch gekennzeichnet,** dass die Anzahl der Ausführungen des echtzeitkonstanten Prozesses (9) als Zählerstand (n, n', m) eines Zeitzählers (13, 14, 15) des Datenträgers (1) protokolliert wird, indem nach jeder Ausführung (S3) des echtzeitkonstanten Prozesses (9) eine Unterbrechung (16) ausgelöst wird (S5, S15) und der Zeitzähler (13, 14, 15) durch eine entsprechende Unterbrechungsroutine (17) inkrementiert wird (S6, S16).

8. Verfahren nach Anspruch 6 und 7, **dadurch gekennzeichnet,** dass eine beginnend mit dem vorgegebenen Ereignis verstrichene Echtzeitspanne bestimmt wird, indem der aktuelle Zählerstand (n, n', m) eines Zeitzählers (13, 14, 15) mit der konstanten Ausführungsdauer (t) des echtzeitkonstanten Prozesses (9) multipliziert wird.

9. Verfahren nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet,** dass eine Ausführung (S3) des echtzeitkonstanten Prozesses (9) fortlaufend sequentiell wiederholt wird (S4), sobald der Datenträger (1) eingeschaltet wird (S1), und die Anzahl der Ausführungen (S3) des echtzeitkonstanten Prozesses (9) als Zählerstand (n) eines Betriebszeitzählers (13) des Datenträgers (1) protokolliert wird (S5, S6).

10. Verfahren nach Anspruch 9, **dadurch gekennzeichnet,** dass zum Inkrementieren (S6) des Zählerstands (n) des Betriebszeitzählers (13) eine Unterbrechung (16) ausgelöst wird (S5) und der Zählerstand (n) des Betriebszeitzählers (13) durch eine entsprechende Unterbrechungsroutine (17) inkrementiert wird

(S6), wobei die Unterbrechung (16) auch in einem Stromsparmodus des Datenträgers (1) auslösbar ist.

11. Verfahren nach Anspruch 9 oder 10, **dadurch gekennzeichnet**, dass von dem Betriebszeitzähler (13) eine Vielzahl von weiteren Zeitzählern (15) abgeleitet werden kann (S9), deren jeweilige Zählerstände (n') basierend auf dem Zählerstand (n) des Betriebszeitzählers (13) aktualisiert werden (S10).

12. Verfahren nach einem der Ansprüche 9 bis 11, **dadurch gekennzeichnet**, dass der Betriebszeitzähler (13) mit einem externen Zeitsynchronisationssignal (23) einer externen Kommunikationsvorrichtung (25) synchronisiert wird (S8).

13. Verfahren nach einem der Ansprüche 9 bis 12, **dadurch gekennzeichnet**, dass ein Betriebszeitsignal (24) an eine externe Kommunikationsvorrichtung (25) gesendet wird, das die sich aus einer Multiplikation des aktuellen Zählerstands (n) des Betriebszeitzählers (13) mit der Ausführungsdauer (t) des echtzeitkonstanten Prozesses (9) ergebende Betriebszeit ($n*t$) des Datenträgers (1) angibt (S7).

14. Verfahren nach einem der Ansprüche 9 bis 13, **dadurch gekennzeichnet**, dass bei Überschreiten eines vorgegebenen Zählerstandes (s) eines Zeitzählers (13, 14, 15) ein Benachrichtigungssignal (24) an eine externe Kommunikationsvorrichtung (25) gesendet wird (S18), das angibt, dass der betreffende Zeitzähler (13, 14, 15) den vorgegebenen Zählerstand (s) überschritten hat.

15. Verfahren nach Anspruch 13 oder 14, **dadurch gekennzeichnet**, dass das Benachrichtigungssignal (24) und/oder das Betriebszeitsignal (22) über eine gesicherte Kommunikationsverbindung und/oder verschlüsselt und/oder signiert an die externe Kommunikationsvorrichtung (25) gesendet wird (S7, S18).

16. Verfahren nach einem der Ansprüche 1 bis 15, **dadurch gekennzeichnet**, dass der Datenträger (1) während einer fortlaufend sequentiellen Ausführung (S3, S4) des echtzeitkonstanten Prozesses (9) kontinuierlich mit einer Versorgungsspannung (Vcc) und einem Taktsignal (CLK) versorgt wird.

17. Verfahren nach einem der Ansprüche 1 bis 16, **dadurch gekennzeichnet**, dass das Verfahren auf einem manipulationssicheren Datenträger (1) ausgeführt wird, insbesondere auf einer Smart Card.

18. Portabler Datenträger (1) umfassend zumindest einen Speicher (4), einen Prozessor (2) zum Ausführen einer auf dem Datenträger (1) vorliegenden Programmroutine (8) als Prozess (9) und eine Kommunikationseinrichtung (12) zur Datenkommunikation mit einer externen Kommunikationsvorrichtung (25) über eine Kommunikationsschnittstelle (6) des Datenträgers (1), **dadurch gekennzeichnet**, dass die Programmroutine (8) ausgestaltet ist, von dem Prozessor (2) als echtzeitkonstanter Prozess (9) mit einer im wesentlichen konstanten Ausführungsdauer (t) ausgeführt zu werden, und durch eine Echtzeitsteuerung (10), die eingerichtet ist, die Ausführung der Programmroutine (8) als echtzeitkonstanter Prozess (9) durch den Prozessor (2) zu bewirken und eine Echtzeitspanne als Vielfaches der Ausführungsdauer (t) des echtzeitkonstanten Prozesses (9) zu bestimmen.

19. Datenträger (1) nach Anspruch 18, **dadurch gekennzeichnet**, dass die Programmroutine (8) ausgestaltet ist, bei einer Ausführung durch den Prozessor (2) als echtzeitkonstanter Prozess (9) nicht auf den zumindest einen Speicher (4) des Datenträgers (1) zuzugreifen.

20. Datenträger (1) nach Anspruch 18 oder 19, **dadurch gekennzeichnet,** dass die Programmroutine (8) ausgestaltet ist, bei ihrer Ausführung als echtzeitkonstanter Prozess (9) durch den Prozessor (2) zumindest eine Zufallszahl zu erzeugen.

21. Datenträger (1) nach einem der Ansprüche 18 bis 20, **gekennzeichnet durch** eine Überwachungseinrichtung (11), die eingerichtet ist, ein Auslösesignal (18) an die Echtzeitsteuerung (10) zu senden, sobald der Prozessor (2) keinen Prozess ausführt, und ein Beendigungssignal (19) an die Echtzeitsteuerung (10) zu senden, sobald der Prozessor (2) einen von dem echtzeitkonstanten Prozess (9) verschiedenen Prozess ausführt, und dadurch, dass die Echtzeitsteuerung (10) eingerichtet ist, bei Empfang des Auslösesignals (18) die Programmroutine (8) als echtzeitkonstanten Prozess (9) durch den Prozessor (2) solange fortlaufend sequentiell wiederholend auszuführen, bis die Echtzeitsteuerung (10) ein Beendigungssignal (19) empfängt.

22. Datenträger (1) nach Anspruch 21, **dadurch gekennzeichnet**, dass die Echtzeitsteuerung (10) eingerichtet ist, die fortlaufend sequentiell wiederholte Ausführung der Programmroutine (8) als echtzeitkonstanten Prozess (9) durch den Prozessor (2) zwischen einem Senden einer Antwortnachricht (20) durch die Kommunikationseinrichtung (12) an die externe Kommunikationsvorrichtung (25) und einem Empfangen einer nächsten Anfragenachricht (21) von der externen Kommunikationsvorrichtung (25) durch die Kommunikationseinrichtung (12) zu bewirken.

23. Datenträger (1) nach einem der Ansprüche 18 bis 20, **gekennzeichnet** durch eine Überwachungseinrichtung (11), die eingerichtet ist, bei Eintreten eines vorgegebenen Ereignisses auf dem Datenträger (1) ein Auslösesignal (18) an die Echtzeitsteuerung (10) zu senden, und dadurch, dass die Echtzeitsteue-

rung (10) eingerichtet ist, die Programmroutine (8) bei Empfang des Auslösesignals (18) fortlaufend sequentiell wiederholend als echtzeitkonstanten Prozess (9) durch den Prozessor (2) auszuführen.

24. Datenträger (1) nach einem der Ansprüche 21 bis 23, **dadurch gekennzeichnet**, dass in dem zumindest einen Speicher (4) des Datenträgers (1) ein Zeitzähler (13, 14, 15) eingerichtet ist, dessen Zählerstand (n, m) eine Anzahl der Ausführungen der Programmroutine (8) als echtzeitkonstanten Prozess (9) wiedergibt, und der Datenträger (1) eingerichtet ist, nach jeder Ausführung des echtzeitkonstanten Prozesses (9) eine Unterbrechung (16) auszulösen und eine entsprechende Unterbrechungsroutine (17) auszuführen, die den Zählerstand (n, m) des Zeitzählers (13, 15) inkrementiert.

25. Datenträger (1) nach Anspruch 23 und 24, **dadurch gekennzeichnet**, dass die Echtzeitsteuerung (10) eingerichtet ist, eine beginnend mit einem Empfang des Auslösesignals (18) verstrichene Echtzeitspanne zu bestimmen, indem der aktuelle Zählerstand (n, n', m) des Zeitzählers (13, 14, 15) ausgelesen und mit der konstanten Ausführungsdauer (t) des echtzeitkonstanten Prozesses (9) multipliziert wird.

26. Datenträger (1) nach einem der Ansprüche 18 bis 20, **dadurch gekennzeichnet**, dass in dem zumindest einen Speicher (4) des Datenträgers (1) ein Betriebszeitzähler (13) eingerichtet ist, dessen Zählerstand (n) eine Anzahl der Ausführungen der Programmroutine (8) als echtzeitkonstanter Prozess (9) durch den Prozessor (2) seit einem Einschalten des Datenträgers (1) wiedergibt, und dass die Echtzeitsteuerung (10) eingerichtet ist, die Programmroutine (8) fortlaufend sequentiell wiederholend als echtzeitkonstanten Prozess (9) durch den Prozessor (2) auszuführen, sobald der Datenträger (1) eingeschaltet wird, wobei der Datenträger (1) eingerichtet ist, den Zählerstand (n) des Betriebszeit-

zählers (13) entsprechend der Anzahl der Ausführungen der Programmroutine (9) zu inkrementieren.

27. Datenträger (1) nach Anspruch 26, **dadurch gekennzeichnet**, dass der Datenträger (1) eingerichtet ist, zum Inkrementieren des Zählerstands (n) des Betriebszeitzählers (13) nach jeder Ausführung des echtzeitkonstanten Prozesses (9) eine Unterbrechung (16) auszulösen und eine entsprechende Unterbrechungsroutine (17) auszuführen, die eingerichtet ist, den Zählerstand (n) des Betriebszeitzählers (13) zu inkrementieren, wobei der Datenträger (1) derart eingerichtet ist, dass die Unterbrechung (16) auch in einem Stromsparmodus des Datenträgers (1) auslösbar ist.

28. Datenträger (1) nach Anspruch 26 oder 27, **dadurch gekennzeichnet**, dass die Echtzeitsteuerung (10) eingerichtet ist, in dem Speicher (4) zumindest einen von dem Betriebszeitzähler (13) abgeleiteten weiteren Zeitzähler (14) einzurichten und einen Zählerstand (n') des zumindest einen abgeleiteten Zeitzählers (15) basierend auf dem aktuellen Zählerstand (n) des Betriebszeitzählers (13) zu aktualisieren.

29. Datenträger (1) nach einem der Ansprüche 26 bis 28, **dadurch gekennzeichnet**, dass der Betriebszeitzähler (1) und/oder der zumindest eine weitere Zeitzähler (15) als persistente Datenobjekte in einem nicht-flüchtigen Speicher (4) des Datenträgers (1) eingerichtet sind.

30. Datenträger (1) nach einem der Ansprüche 26 bis 29, **dadurch gekennzeichnet**, dass die Echtzeitsteuerung (10) eingerichtet ist, ein Zeitsynchronisationssignal (23) von einer externen Kommunikationsvorrichtung (25) über die Kommunikationsschnittstelle (6) zu empfangen und den Betriebszeitzähler (13) mit dem externen Zeitsynchronisationssignal (23) zu synchronisieren.

31. Datenträger (1) nach einem der Ansprüche 26 bis 30, **dadurch gekennzeichnet**, dass die Echtzeitsteuerung (10) eingerichtet ist, den Zählerstand (n) des Betriebszeitzählers (13) zu überwachen, die Betriebszeit des Datenträgers (1) durch Multiplikation des Zählerstands (n) des Betriebszeitzählers (13) mit der Ausführungsdauer (t) der als echtzeitkonstanter Prozess (9) ausgeführten Programmroutine (8) zu ermitteln und über die Kommunikationseinrichtung (12) ein Betriebszeitsignal (22) an eine externe Kommunikationsvorrichtung (12) zu senden, das die Betriebszeit ($n*t$) des Datenträgers (1) angibt.

32. Datenträger (1) nach einem der Ansprüche 26 bis 31, **dadurch gekennzeichnet**, dass die Echtzeitsteuerung (10) eingerichtet ist, den Zählerstand (n, n', m) zumindest eines der im Speicher (4) des Datenträgers (1) eingerichteten Zeitzählers (13, 14, 15) zu überwachen und bei Überschreitung eines vorgegebenen Zählerstandes (s) durch einen der überwachten Zeitzähler (13, 14, 15) über die Kommunikationseinrichtung (12) ein Benachrichtigungssignal (24) an eine externe Kommunikationsvorrichtung (25) zu senden, das angibt, dass der betreffende Zeitzähler (13, 14, 15) den vorgegebene Zählerstand (s) überschritten hat.

33. Datenträger (1) nach Anspruch 31 oder 32, **dadurch gekennzeichnet**, dass die Kommunikationseinrichtung (12) eingerichtet ist, eine gesicherte Kommunikationsverbindung zu der externen Kommunikationsvorrichtung (25) aufzubauen und das Betriebszeitsignal (22) und/oder das Benachrichtigungssignal (24) über die gesicherte Kommunikationsverbindung an die externe Kommunikationsvorrichtung (25) zu senden.

34. Datenträger (1) nach Anspruch 33, **dadurch gekennzeichnet**, dass die Kommunikationseinrichtung (12) eingerichtet ist, das Betriebszeitsignal (22)

und/oder das Benachrichtigungssignal (24) verschlüsselt und/oder signiert an die externe Kommunikationsvorrichtung (25) zu senden.

35. Datenträger (1) nach einem der Ansprüche 18 bis 34, **dadurch gekennzeichnet**, dass der Datenträger (1) ein manipulationssicherer Datenträger (1) ist, insbesondere eine SmartCard.

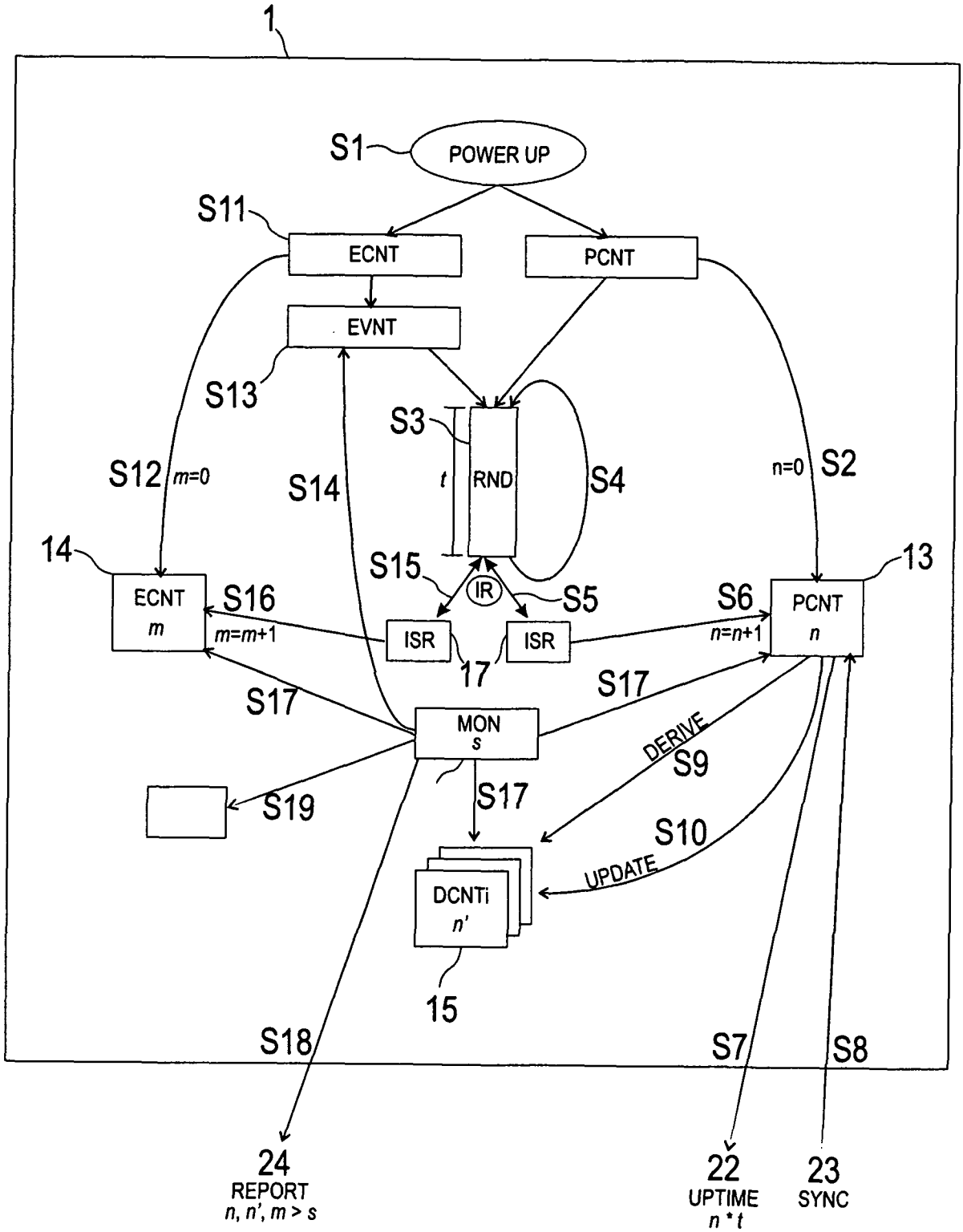

1
S1
POWER UP
S11
ECNT
PCNT
EVNT
S13
S3
t
RND
S4
S12
m=0
S14
n=0
S2
14
S15
IR
S5
13
ECNT
m
S16
m=m+1
ISR
ISR
S6
n=n+1
PCNT
n
17
S17
S17
MON
s
DERIVE
S9
S19
S17
S10
UPDATE
DCNTi
n'
15
S18
S7
S8
24
REPORT
n, n', m > s
22
UPTIME
n * t
23
SYNC

Fig.1

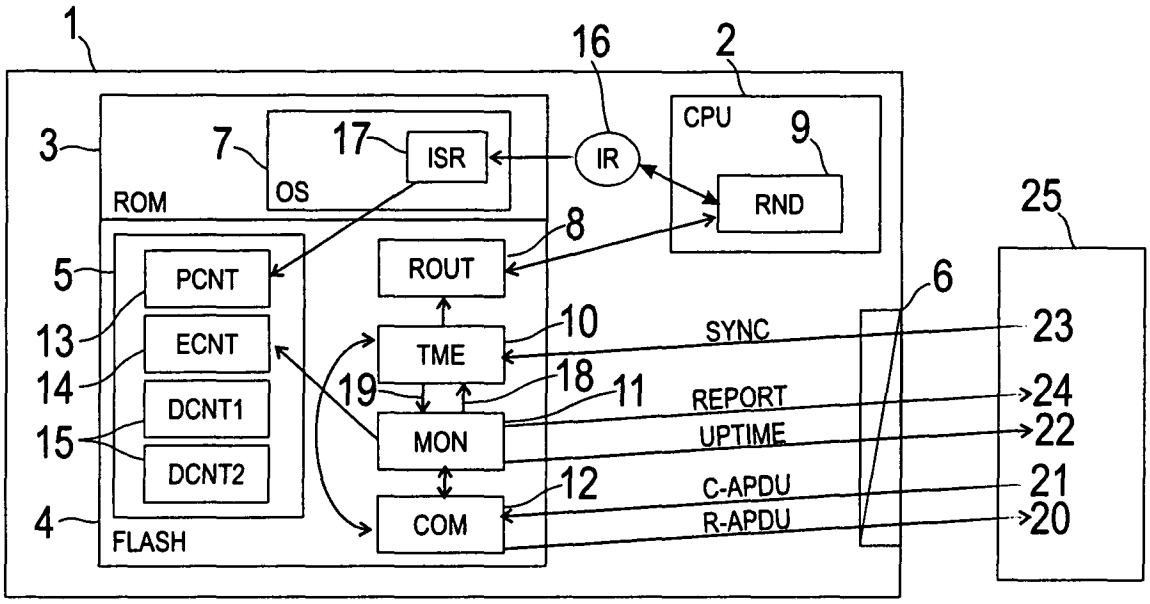

1
16
2
3
7
17
ISR
IR
CPU
9
ROM
OS
RND
25
8
5
PCNT
ROUT
6
13
ECNT
TME
10
SYNC
23
14
DCNT1
19
18
11
REPORT
24
15
DCNT2
MON
UPTIME
22
12
C-APDU
21
4
FLASH
COM
R-APDU
20

Fig.2