(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
13. Februar 2014 (13.02.2014)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2014/023394 A1

(51) Internationale Patentklassifikation:
G06F 9/445 (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2013/002152

(22) Internationales Anmeldedatum:
19. Juli 2013 (19.07.2013)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2012 015 573.5
7. August 2012 (07.08.2012) DE

(71) Anmelder: **GIESECKE & DEVRIENT GMBH** [DE/DE]; Prinzregentenstrasse 159, 81677 München (DE).

(72) Erfinder: **RUDOLPH, Jens**; Eisnergutbogen 30, 80639 München (DE). **RÖSNER, Martin**; Pfarrer-Kaiser-Ring 29, 83527 Haag in Oberbayern (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, 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, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, 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)*

Veröffentlicht:

— *mit internationalem Recherchenbericht (Artikel 21 Absatz 3)*

(54) **Title**: METHOD FOR ACTIVATING AN OPERATING SYSTEM IN A SECURITY MODULE

(54) **Bezeichnung** : VERFAHREN ZUM AKTIVIEREN EINES BETRIEBSSYSTEMS IN EINEM SICHERHEITSMODUL

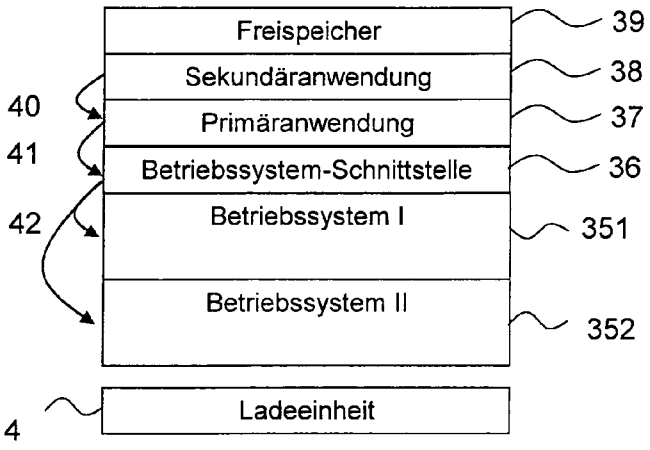

Fig. 3

39 Free memory
38 Secondary application
37 Primary application
36 Operating system interface
351 Operating system I
352 Operating system II
4 Loading unit

(57) **Abstract**: The invention relates to a method for activating an operating system (35) in a security module (3), wherein the security module (3) is operational either using a first operating system (351) or using a second operating system (352). The method comprises the following steps: the security module (3) is operated using the first operating system (351) and the security module (3) is converted (6) from the first operating system (351) to the second operating system (352). In particular, a primary application (37) introduced into the security module (3) uses an operating system interface (36) to access the respective operating system (35). The concept of the invention furthermore comprises a security module and also the use of a security module in a terminal.

(57) **Zusammenfassung**: Die Erfindung betrifft ein Verfahren zum Aktivieren eines Betriebssystems (35) in einem Sicherheitsmodul (3), wobei das Sicherheitsmodul (3) entweder mittels eines ersten Betriebssystems (351) oder mittels eines zweiten Betriebssystems (352) betriebsfähig ist. Das Verfahren umfasst die Schritte: Betreiben des Sicherheitsmoduls (3) mittels des ersten Betriebssystems (351) und Umsetzen (6) des Sicherheitsmoduls (3) vom ersten Betriebssystem (351) auf das zweite Betriebssystem (352). Insbesondere greift

eine

[Fortsetzung auf der nächsten Seite]

WO 2014/023394 A1

in das Sicherheitsmodul (3) eingebrachte Primäranwendung (37) mittels einer Betriebs-Systemschnittstelle (36) auf das jeweilige Betriebssystem (35) zu. Der Erfindungsgedanke umfasst weiterhin ein Sicherheitsmodul sowie die Verwendung eines Sicherheitsmoduls in einem Endgerät.

Verfahren zum Aktivieren eines Betriebssystems in einem Sicherheitsmodul

Die Erfindung betrifft ein Verfahren zum Aktivieren eines Betriebssystems in einem Sicherheitsmodul, ein Sicherheitsmodul sowie die Verwendung eines Sicherheitsmoduls in einem Endgerät.

Sicherheitsmodule weisen Systemressourcen auf, insbesondere Datenschnittstellen zur Dateneingabe bzw. Datenausgabe, eine oder mehrere zentrale Recheneinheiten CPU, Koprozessoren, flüchtige Speicherbereiche als Arbeitsspeicher und nichtflüchtige Speicherbereiche insbesondere EEPROM, ROM und/oder FLASH. Auf dem Sicherheitsmodul werden Anwendungen ausgeführt, die während ihrer Ausführung auf die Systemressourcen des Sicherheitsmoduls zugreifen. Dieser Zugriff der Anwendungen auf die Systemressourcen wird von einem Betriebssystem des Sicherheitsmoduls verwaltet. Das Betriebssystem des Sicherheitsmoduls bildet somit eine Schnittstelle zwischen den Systemressourcen und den jeweils auszuführenden Anwendungen auf dem Sicherheitsmodul.

Werden Fehler im Betriebssystem entdeckt oder wird festgestellt, dass eine bestimmte Funktionalität im Betriebssystem nicht enthalten ist, beispielsweise eine Funktion, eine Methode oder eine Programmcodebibliothek, so können fehlende oder korrigierte Betriebssystemcodeteile, sogenannte Patches, nachgeladen werden. Dabei werden Einsprungadressen definiert, an denen - anstelle des fehlerhaften/fehlenden Betriebssystemcodes - der Patch ausgeführt wird. Mittels definierter Rücksprungadressen im Patch kann anschließend wieder zum Ausgangspunkt einer Anwendung zurückgekehrt werden.

In der DE 10 2007 003 580A1 ist das Patchen eines tragbaren Datenträgers beschrieben, wobei hierbei der Patch in Form eines ausführbaren Anwendungscodes in den Datenträger nachgeladen und ausgeführt wird, was eine Installation von Betriebssystemteilen während des Betriebs des tragbaren Datenträgers ermöglicht.

Dieses Patchen ist aufwendig und führt nur zur Korrektur bzw. Erweiterung von kleinen Teilen des Betriebssystems. Daher wird von Zeit zu Zeit eine neue Version des Betriebssystems erstellt. Sicherheitsmodule, die bereits in Betrieb sind werden dann entweder ausgetauscht oder es wird auf das Aktualisieren des Betriebssystems verzichtet.

Es ist wünschenswert, das Betriebssystem in einem Sicherheitsmodul stets auf dem neuesten Entwicklungsstand zu halten. Auf diese Weise können zusätzliche Funktionen, Umstrukturierungen im Betriebssystemcode und Leistungssteigerungen des Sicherheitsmoduls erzielt werden. Insbesondere werden die in der Vergangenheit entdeckten Fehler in der älteren Version des Betriebssystems korrigiert. Da diese Betriebssystemaktualisierung umfangreich ist, ist dies mit dem erwähnten Patchen nicht ohne erheblichen Rechenleistungsverlust des Sicherheitsmoduls möglich.

Aus der DE 10 336 568 A1 ist bekannt, ein Notfallbetriebssystem in einer Chipkarte zu implementieren, sodass beim Auftreten eines größeren Fehlers beim Betrieb der Chipkarte mit dem normalen Betriebssystem immerhin eine Minimalfunktionalität der Chipkarte gewährleistet ist. Dabei werden allerdings viele Funktionen im Notfallbetriebssystem nicht angeboten, so dass der Nutzer der Chipkarte massiv eingeschränkt und bemüht ist, die Chipkarte schnellstmöglich auszutauschen.

Aus der US 7,011,252 B1 ist bekannt, zwei Betriebssysteme in den permanenten nichtflüchtigen Speicherbereich (ROM) einer Chipkarte einzubringen. Anhand der verwendeten Datenschnittstelle wird entweder das eine oder das andere Betriebssystem zur Ausführung einer Anwendung verwendet. Die Betriebssysteme sind dabei ebenfalls nicht aktualisierbar, d.h. Fehler in einem der Betriebssysteme müssen weiterhin mittels Patches korrigiert werden.

Der Erfindung liegt die Aufgabe zugrunde, das Betriebssystem eines Sicherheitsmoduls ersetzen zu können. Dabei soll das Sicherheitsmodul jederzeit betriebsfähig sein, insbesondere soll ein Löschen des alten Betriebssystems vor dem Aktivieren eines neueren/anderen Betriebssystems nicht möglich sein, um auf Anwendercode und Daten im Sicherheitsmodul jederzeit zugreifen zu können. Insbesondere ist das Sicherheitsmodul zum Zeitpunkt des Ersetzens bereits in Verwendung. Insbesondere soll das Ersetzen unkompliziert und ohne Aufwand ermöglicht werden, sodass der im Sicherheitsmodul bereits eingebrachte Anwendercode oder die bereits eingebrachten Daten nicht an das neuere Betriebssystem adaptiert bzw. angepasst werden müssen.

Die Aufgabe der Erfindung wird durch die in den nebengeordneten unabhängigen Patentansprüchen beschriebenen Maßnahmen gelöst. Vorteilhafte Ausgestaltungen sind in den jeweils abhängigen Ansprüchen beschrieben.

Die Aufgabe wird mit einem erfindungsgemäßen Verfahren zum Aktivieren eines Betriebssystems in einem Sicherheitsmodul gelöst, wobei das Sicherheitsmodul entweder mittels eines ersten Betriebssystems oder mittels eines zweiten Betriebssystems betriebsfähig ist. Dabei wird das Sicherheitsmodul mittels des ersten Betriebssystems betrieben. Anschließend erfolgt ein Um-

setzen bzw. Umschalten des Sicherheitsmoduls vom ersten Betriebssystem auf das zweite Betriebssystem, d.h. das Sicherheitsmodul wird nicht mehr mit dem ersten Betriebssystem, sondern mit dem zweiten Betriebssystem betrieben. Erfindungsgemäß greift eine in das Sicherheitsmodul eingebrachte Primäranwendung mittels einer Betriebssystemschnittstelle auf das jeweilige Betriebssystem zu, sodass die eingebrachte Primäranwendung durch den Schritt des Umsetzens unverändert bleiben kann.

Bei einem Sicherheitsmodul im Sinne der Erfindung handelt es sich um ein in Baugröße und Ressourcenumfang reduziertes Modul, welches eine zentrale Recheneinheit, mindestens eine Datenschnittstelle zur Kommunikation mit einem Endgerät und einen Speicherbereich aufweist. Dieser Speicherbereich ist dergestalt, dass Daten sicher eingebracht sind, wodurch Manipulations- und/oder Missbrauchsversuche zur Entwendung der Daten aus dem Sicherheitsmodul erfolglos bleiben. Die Daten im Sicherheitsmodul dienen beispielsweise der Identifizierung und/oder Authentisierung eines Benutzers an einem Terminal, einem Endgerät oder einem Netzwerk.

Bei dem Sicherheitsmodul handelt es sich beispielsweise um eine Chipkarte, auch Universal Integrated Circuit Card (UICC) oder SIM-Karte, ein elektronisches Identitätsdokument (eID, ePass), einen elektronischen Führerschein, elektronischen Fahrzeugschein oder um eine Bezahlkarte, wie Kredit- bzw. Debitkarte.

Insbesondere ist das Sicherheitsmodul ein Teilnehmeridentitätsmodul zur Authentisierung/Identifizierung eines Teilnehmers in einem mobilen Funknetz mit auf einem Chip gespeicherten maschinenlesbaren Teilnehmeridentitätsdaten des Teilnehmers. Derartige Teilnehmeridentitätsmodule werden mittels Kartenleseeinheiten in einem Endgerät betrieben und können prinzi-

piell aus dem Endgerät entnommen werden, um entweder gegen andere Teilnehmeridentitätsmodule ausgetauscht oder in einem anderen Endgerät betrieben zu werden.

Alternativ handelt es sich bei dem Sicherheitsmodul um einen integralen Bestandteil innerhalb eines Endgeräts, beispielsweise eines fest verdrahteten elektronischen Bausteins. Derartige Sicherheitsmodule werden auch als embedded UICC (eUICC) oder embedded Secure Elements (eSE) bezeichnet. In dieser Bauform sind diese Sicherheitsmodule nicht für eine Entnahme aus dem Endgerät vorgesehen und können prinzipiell nicht einfach ausgetauscht werden.

Alternativ handelt es sich bei dem Sicherheitsmodul um ein Machine-to-Machine-, kurz M2M-, Modul. Diese Module dienen der Fernüberwachung, -kontrolle und -wartung von Endgeräten wie Maschinen, Anlagen und Systemen. Sie können alternativ auch für Zähleinheiten wie Stromzähler, Warmwasserzähler, sogenannte Smart-Meter, verwendet werden.

Alternativ ist das Sicherheitsmodul als eine Softwarekomponente in einem vertrauenswürdigen Teil eines Betriebssystems, einer sogenannten Trusted Execution Environment (TEE) des Endgerätes ausgebildet. Das Sicherheitsmodul ist dann beispielsweise innerhalb einer gesicherten Laufzeitumgebung in Form von darin ablaufenden Programmen, sogenannten Trustlets ausgebildet.

Erfindungsgemäß greift eine Primäranwendung nicht mehr direkt auf das Betriebssystem zu. Stattdessen greift die Primäranwendung mittels einer in das Sicherheitsmodul eingebrachten Betriebssystemschnittstelle auf das Betriebssystem zu. Als Betriebssystemschnittstelle wird auch das Umsetzen der

Verlinkungen auf Systemressourcen vom ersten Betriebssystem auf das zweite Betriebssystem verstanden. Der Schritt des Umsetzens durch das Umsetzen der Verlinkung wird von der Betriebssystemschnittstelle durchgeführt und/oder verwaltet.

Die Betriebssystemschnittstelle ist dabei Zwischenschicht in einem schichtenorientierten Betriebssystem. Sie ist nicht mit einer Hardwareabstraktionsschicht (englisch Hardware Abstraction Layer, HAL) zu verwechseln, da eine HAL eine Schicht zwischen Betriebssystem und der Hardwareschicht ist und dazu dient das Betriebssystem auf unterschiedliche Prozessorarchitekturen anzupassen. Dagegen ist die Betriebssystemschnittstelle eine Schicht zwischen dem Betriebssystem und der Primäranwendung und dient zum Abstrahieren des Betriebssystems gegenüber der Primäranwendung.

Insbesondere wird das Aktivieren des zweiten Betriebssystems durch Umsetzen von Speicheradressverweisen in der Betriebssystemschnittstelle realisiert. Dies hat den Vorteil, dass zwischen den Systemressourcen und den jeweils auszuführenden Anwendungen auf dem Sicherheitsmodul eine abstrahierende Schnittstelle eingeführt wird und somit das jeweilige Betriebssystem von allen Anwendungen auf dem Sicherheitsmodul entkoppelt wird. Somit ist die Primäranwendung unabhängig von dem tatsächlich auf dem Sicherheitsmodul installierten Betriebssystem. Somit kann zwischen dem ersten Betriebssystem und dem zweiten Betriebssystem umgeschaltet werden, ohne dass Aufrufe der Primäranwendung für Systemressourcen des Sicherheitsmoduls angepasst werden müssen.

Das erste und zweite Betriebssystem, beispielsweise ausgestaltet gemäß dem Standard ISO/IEC 7816-4 , ETSI TS 102.221, ETSI TS 101.220, ETSI TS 102.241 oder ETSI TS 102.226, verwaltet dabei weiterhin prinzipiell die Datenbearbei-

tung und Datenübertragung zwischen den einzelnen Systemressourcen des Sicherheitsmoduls, die Datenbearbeitung und Datenübertragung von dem Sicherheitsmodul auf ein in Datenkommunikation befindliches Endgerät bzw. von dem Endgerät auf das Sicherheitsmodul, die Ablaufsteuerung von Befehlskommandos, die Verwaltung der physikalischen Speicheradressen des Speicherbereichs und/oder die Verwaltung und Ausführung der Primäranwendung. Dazu weist das Betriebssystem beispielsweise einen I/O Manager, einen eigenen Kommandointerpreter einen Returncode Manager, einen Betriebssystemkern, einen Ressourcenmanager zur Verwaltung der Hardware und des Speicherbereiches und/oder einen Befehlssatz auf. Weiterführende Informationen zu einem Betriebssystem eines Sicherheitsmoduls können dem Kapitel 13 des „Handbuch der Chipkarten" der Autoren Wolfgang Rankl & Wolfgang Effing in der beim Hanser Verlag erschienen 5. Auflage entnommen werden, auf das hiermit vollumfänglich Bezug genommen wird. Der Fachmann wird erkennen, dass unter den hierin verwendeten Begriff "Betriebssystem" auch eine Firmware fällt, da definitionsgemäß eine Firmware ein proprietäres Betriebssystem ist, welches hardwarenah im Sicherheitsmodul eingebracht ist.

Das erste Betriebssystem unterscheidet sich vom zweiten Betriebssystem beispielsweise in der Version, also einem alternativen Entwicklungsstadium mit Veränderungen und Weiterentwicklungen von zumindest Teilen des Betriebssystems. Alternativ und/oder zusätzlich unterscheidet sich das erste Betriebssystem vom zweiten Betriebssystem in der Variante des Betriebssystems, sodass ein alternativer Funktionsumfang im zweiten Betriebssystem vorhanden ist.

Das Umsetzen bzw. Umschalten von dem ersten auf das zweite Betriebssystem erfolgt bevorzugt innerhalb weniger Taktzyklen des Sicherheitsmoduls.

Dazu weist die Betriebssystemschnittstelle eine Verlinkungstabelle auf, in der die Speicheradressverlinkungen zwischen der Primäranwendung und dem ersten Betriebssystem sowie die Speicheradressverlinkungen zwischen der Primäranwendung und dem zweiten Betriebssystem abgelegt sind. Mittels eines Umschaltkommandos, getriggert durch ein Endgerät, eine entfernte Instanz oder das Sicherheitsmodul selbst, erfolgt ein Umsetzen der Speicheradressen auf das zweite Betriebssystem. Durch den Einsatz einer Verlinkungstabelle erfolgt das Umsetzen innerhalb kürzester Zeit, sodass der Betrieb des Sicherheitsmoduls schnellstmöglich wieder aufgenommen werden kann.

Nach dem Schritt des Umsetzens erfolgt ein Neustart des Sicherheitsmoduls, um den Betrieb des Sicherheitsmoduls mit dem zweiten Betriebssystem zu ermöglichen. Dazu sendet die Betriebssystemschnittstelle beispielsweise ein REFRESH Kommando an ein zum Betrieb benötigtes Endgerät. Alternativ erfolgt endgeräteseitig mit dem Senden eines Umsetzkommandos der Start einer vordefinierten Wartezeitschleife, bei deren Ablauf das Sicherheitsmodul neugestartet wird, ein RESET erfolgt oder kurzzeitig die Betriebsspannung abgeschaltet wird.

In einer bevorzugten Ausgestaltung der Erfindung greift die eingebrachte Primäranwendung nur über die Betriebssystemschnittstelle auf das erste Betriebssystem oder das zweite Betriebssystem zu. Weiterhin ist die Primäranwendung zur Ausführung mindestens einer Sekundäranwendung eingerichtet, wobei die Sekundäranwendung nur mittels der Primäranwendung und der Betriebssystemschnittstelle auf das erste Betriebssystem oder das zweite Betriebssystem zugreifen kann. Bezogen auf das erfindungsgemäße Verfahren wird hiermit eine zweite Abstraktionsebene eingeführt. Dadurch ist eine vollständige Abstrahierung des Betriebssystems von allen Anwendungen

auf dem Sicherheitsmodul erzielt, wodurch auf ein komplett alternatives Betriebssystem umgeschaltet werden kann, ohne eine der Primär- und/oder Sekundäranwendungen anpassen zu müssen.

Es wird somit in vorteilhafter Weise ein betriebssystemunabhängiges Sicherheitsmodul erschaffen, wobei zwar weiterhin ein Betriebssystem zum Betreiben des Sicherheitsmoduls notwendig ist, die genaue Ausgestaltung, Version und/oder Variante jedoch für das spezielle Sicherheitsmodul und die darauf auszuführenden Primär- und/oder Sekundäranwendungen unrelevant sind.

In einer bevorzugten Ausgestaltung ist die Primäranwendung eine virtuelle Maschine, insbesondere eine Java Card Virtuelle Maschine, kurz JCVM. Mit dieser Primäranwendung ist es möglich, Sekundäranwendungen auf dem Sicherheitsmodul weiter zu abstrahieren und diese auf unterschiedlichen Sicherheitsmodulplattformen ausführen zu können. Es ist bei Sicherheitsmodulen bekannt, dass Sekundäranwendungen, insbesondere programmierte Java-Applikationen (Applets, Trustlets), ein Dateisystem (MF, DF) mit Daten in Dateien (EF), Sicherheitszonen (Security Domains; SD), Programmbibliotheken (API) nur auf die Primäranwendung und insbesondere nicht auf das Betriebssystem zugreifen. Ist die Primäranwendung eine virtuelle Maschine, kann die Betriebssystemschnittstelle auch als ein Application Programming Interface, kurz API, ausgestaltet sein, welche das Umschalten von den Adressen zur Systemressourcenverwaltung durch das erste Betriebssystem auf das zweite Betriebssystem umsetzt.

In einer alternativen Ausgestaltung ist eine virtuelle Maschine Teil des Betriebssystems und wird im Rahmen des Aktivierens des zweiten Betriebssystems durch eine neuere und/oder verbesserte Version der virtuellen Maschine ersetzt. In dieser Ausgestaltung können zusätzlich Primäranwendun-

gen auf dem Sicherheitsmodul eingebracht sein. Sekundäranwendungen und die ggf. zusätzlichen Primäranwendungen werden von der Betriebssystemschnittstelle abstrahiert und sind nach dem Aktivieren des zweiten Betriebssystems unverändert aufrufbar.

In einer Ausgestaltung ist die Primäranwendung ein nativer Dienst, beispielsweise ein Kryptoalgorithmus, wie DES oder AES-Algorithmus oder ein alternativer nativer Programmcode, bei dem ausführbarer Code direkt von dem Betriebssystem zu verarbeiten ist. Diese Primäranwendungen greifen nunmehr nur auf die Betriebssystemschnittstelle zu, welche wiederum auf das jeweilige Betriebssystem zugreift.

In einer bevorzugten Ausgestaltung wird das zweite Betriebssystem vor dem Schritt des Umsetzens in einen Speicherbereich des Sicherheitsmoduls geladen. Zum Laden des zweiten Betriebssystems ist das Sicherheitsmodul mit dem ersten Betriebssystem betriebsfähig. Das zweite Betriebssystem wird dabei insbesondere über eine Datenschnittstelle des Sicherheitsmoduls in den Speicherbereich geladen. Somit kann das zweite Betriebssystem auch zu einem Zeitpunkt nach der Fertigstellung des Sicherheitsmoduls, d.h. im Feld mit dem zweiten Betriebssystem ausgestattet werden.

Das zweite Betriebssystem wird dabei beispielsweise in Form von nativem Code in einen reservierten Speicherbereich, bspw. in ein dafür vorgesehenes EF geladen. Er ist prinzipiell relokatibel, d.h. ein Umspeichern in einen anderen Speicherbereich ist möglich. Daher weist das zweite Betriebssystem zum Zeitpunkt des Ladens vorzugsweise noch keine festen physikalischen Adressen, sondern lediglich relative Adressen auf. Erfindungsgemäß setzt die Betriebssystemschnittstelle die Adressen des zweiten Betriebssystems dann entsprechend um.

Dazu ist das Sicherheitsmodul mittels eines Endgeräts betriebsfähig, um das zweite Betriebssystems zu erhalten. Bei einem Endgerät im Sinn der Erfindung handelt es sich insbesondere um ein Gerät oder eine Gerätekomponente, welches Mittel zur Kommunikation mit einem Kommunikationsnetzwerk aufweist, um das zweite Betriebssystem zu erhalten. Beispielsweise ist ein mobiles Endgerät wie ein Smart Phone, ein Tablet-PC, ein Notebook, ein PDA unter diesen Begriff zu fassen. Unter dem Endgerät können beispielsweise auch Multimediaendgeräte wie digitale Bilderrahmen, Audiogeräte, Fernsehgeräte, E-Book-Reader verstanden werden, die ebenfalls Mittel zur Kommunikation mit einem Kommunikationsnetzwerk aufweisen. Beispielsweise umfasst der Begriff Endgeräte auch jegliche Art von Maschinen, Automaten, Fahrzeuge, Einrichtungen, Smart-Meter, die Mittel, insbesondere Mobilfunkmodems, zur Kommunikation mit dem Kommunikationsnetzwerk aufweisen. Das zweite Betriebssystem kann insbesondere über eine Luftschnittstelle, wie OTA, OTI und/oder WLAN an das Endgerät übermittelt werden. Alternativ kann das zweite Betriebssystem über eine kontaktbehaftete Schnittstelle an das Endgerät übermittelt werden.

Das Laden in das Sicherheitsmodul erfolgt insbesondere über eine Ladeeinheit, auch Urlader oder Bootloader genannt, des Sicherheitsmoduls. Dazu wird ein sicherer Speicherbereich des Sicherheitsmoduls zum Ablegen des zweiten Betriebssystems ausgewählt. Der Speicherbereich in dem Sicherheitsmodul ist bevorzugt für das zweite Betriebssystem reserviert, sodass ein Aktualisieren des Sicherheitsmoduls ohne Löschen von ggf. anwenderspezifischen Daten erfolgen kann. Mittels eines Fehlererkennungscodes, einer Prüfsumme, einer Checksumme oder EDC bzw. mit einer digitalen Signatur ist das zweite Betriebssystem abgesichert. Damit wird das zweite Betriebssystem auf Datenintegrität geprüft. Zum Zeitpunkt des Ladens ist das erste Betriebssystem des Sicherheitsmoduls aktiviert.

Das Laden in das Sicherheitsmodul erfolgt alternativ über eine Anwendung des Endgeräts. Zum Zeitpunkt des Ladens ist das erste Betriebssystem des Sicherheitsmoduls aktiviert.

In einer Weiterbildung der Erfindung wird das zweite Betriebssystem vor dem Schritt des Umsetzens bzw. Umschaltens in einen Speicherbereich des Sicherheitsmoduls in verschlüsselter Form geladen und dort zunächst auf Plausibilität geprüft. Die Plausibilitätsprüfung erfolgt insbesondere mittels Prüfen eines Fehlererkennungscode (=EDC oder Checksumme), sodass der Transport und auch das Laden des zweiten Betriebssystems abgesichert erfolgt. Das Integrieren von Schad- und/oder Spionagesoftware in das zweite Betriebssystem ist somit sicher unterbunden. Das Entschlüsseln erfolgt mittels in das Sicherheitsmodul eingebrachter individueller kryptografischer Schlüssel. Diese Schlüssel werden vor dem Laden des Betriebssystems in das Sicherheitsmodul unter Authentisierung/Identifizierung des Sicherheitsmoduls eingebracht.

Nach dem Entschlüsseln erfolgt eine Analyse des zweiten Betriebssystems durch die Betriebssystemschnittstelle, insbesondere werden Speicheradressverlinkungen in einer Verlinkungstabelle abgelegt.

Nach dem erfolgreichen Umsetzen und Aktivieren des zweiten Betriebssystems erfolgt das Senden einer Bestätigungsinformation an eine entfernte Instanz. Dabei wird bereits das zweite Betriebssystem unter Verwendung der Betriebssystemschnittstelle verwendet. Somit wird die entfernte Instanz darüber informiert, welches Sicherheitsmodul mit welchem Betriebssystem betrieben wird, um ggf. später weitere Aktualisierungen durchführen zu können.

In einer Ausgestaltung der Erfindung wird nach dem erfolgreichen Aktivieren des zweiten Betriebssystems das erste Betriebssystem gelöscht. Dadurch wird Speicherbereich im Sicherheitsmodul freigegeben, der für Primär- und/oder Sekundäranwendungen verwendet werden kann. Alternativ bleibt der Speicherplatz reserviert, um zukünftige Betriebssysteme nachladen zu können.

In einer bevorzugten Ausgestaltung analysiert die Betriebssystemschnittstelle vor dem Schritt des Umsetzens das erste Betriebssystem auf Speicheradressverweise zwischen der Primäranwendung und dem ersten Betriebssystem. Diese analysierten Speicheradressverweise werden in einer Verlinkungstabelle abgelegt. Somit ist sichergestellt, dass die Betriebssystemschnittstelle alle Speicheradressen des ersten Betriebssystems auf Speicheradressen des zweiten Betriebssystems umverlinken kann.

Erfindungsgemäß ist auch ein Sicherheitsmodul mit einer zentralen Recheneinheit, einem Speicherbereich und einer Datenschnittstelle vorgesehen, wobei im Speicherbereich ein erstes Betriebssystem und zumindest eine Primäranwendung abgelegt sind und wobei das Sicherheitsmodul mit dem ersten Betriebssystem betriebsfähig ist. Das Sicherheitsmodul weist eine Betriebssystemschnittstelle mit direktem Zugriff auf das erste Betriebssystem auf. Die Primäranwendung greift indirekt über die Betriebssystemschnittstelle auf das erste Betriebssystem zu.

Bevorzugt weist das Sicherheitsmodul im Speicherbereich ein zweites Betriebssystem auf, wobei die Betriebssystemschnittstelle direkt auf das zweite Betriebssystem zugreift. Das Sicherheitsmodul weist zusätzlich einen Umsetzer zum Umsetzen bzw. Umschalten zwischen dem ersten Betriebssystem

und dem zweiten Betriebssystem auf, wobei die Primäranwendung unverändert bleibt.

Im Erfindungsgrundgedanken ist weiterhin die Verwendung eines Sicherheitsmoduls in einem Endgerät, wobei das zweite Betriebssystem von einer entfernten Instanz über ein mobiles Kommunikationsnetz bereitgestellt ist.

Ein Kommunikationsnetzwerk im Sinn der vorliegenden Erfindung ist eine technische Einrichtung, auf der die Übertragung von Signalen unter Identifizierung und/oder Authentisierung des Kommunikationsteilnehmers stattfindet, wodurch Dienste angeboten werden. Insbesondere wird in dieser Erfindung unter einem Mobilfunknetz beispielsweise das „Global System for Mobile Communications", kurz GSM als Vertreter der zweiten Generation oder das „General Packet Radio Service", kurz GPRS bzw. „Universal Mobile Telecommunications System", kurz UMTS als Vertreter der dritten Generation oder das „Long Term Evolution", kurz LTE, als Vertreter der vierten Generation verstanden.

Nachfolgend wird anhand von Figuren die Erfindung bzw. weitere Ausführungsformen und Vorteile der Erfindung näher erläutert, wobei die Figuren lediglich Ausführungsbeispiele der Erfindung beschreiben. Gleiche Bestandteile in den Figuren werden mit gleichen Bezugszeichen versehen. Die Figuren sind nicht als maßstabsgetreu anzusehen, es können einzelne Elemente der Figuren übertrieben groß bzw. übertrieben vereinfacht dargestellt sein.

Es zeigen:

Figur 1 Ein Blockschaltbild eines Sicherheitsmoduls nach dem Stand der Technik

Figur 2 Eine Darstellung der schichtenorientierten Softwarestruktur eines Sicherheitsmoduls

Figur 3 Eine vereinfachte Darstellung eines Speicherbereichs eines erfindungsgemäßen Sicherheitsmoduls mit zwei Betriebssystemen und einer Betriebssystemschnittstelle

Figur 4 Eine erfindungsgemäße Verlinkungstabelle innerhalb des Sicherheitsmoduls

Figur 5 Eine detaillierte Schichtendarstellung eines erfindungsgemäßen Sicherheitsmoduls mit zwei Betriebssystemen und der Betriebssystemschnittstelle

Figur 6 Ein erfindungsgemäßes Verfahrensablaufdiagramm

Figur 1 zeigt ein Blockschaltbild eines Sicherheitsmoduls 3 gemäß dem Stand der Technik. Das Sicherheitsmodul 3 weist verschiedene Systemressourcen auf, beispielsweise eine Datenschnittstelle 31 zur Datenein- und Datenausgabe. Die Datenschnittstelle 31 ist beispielsweise eine Nahfeldkommunikationsschnittstelle gemäß einer der ISO/IEC 14443, ISO/IEC 15693, ISO/IEC 18092 bzw. Bluetooth gemäß IEEE 802.15.1 bzw. ein direktes lokales Funknetz, kurz WLAN gemäß IEEE 802.11 bzw. eine Infrarot-Übertragung bzw. Wireless USB gemäß ISO/IEC 26907 bzw. eine Single Wire Protokollschnittstelle. Alternativ und/oder zusätzlich ist die Datenschnittstelle 31 kontaktbehaftet ausgestaltet, beispielsweise mittels ISO/IEC 7816, USB, Firewire, MMC, SD Spezifikation etc.

Ein Speicherbereich 33 als weitere Systemressource mit einem flüchtigen Speicherbereich RAM, einem permanent-nichtflüchtigen Speicherbereich ROM sowie einem semipermanent-nichtflüchtigen Speicherbereich EEPROM oder FLASH ist ebenfalls im Sicherheitsmodul 3 vorgesehen. Gemäß Stand der Technik ist im ROM zumindest ein Betriebssystem 35 abgelegt, gemäß dem einleitend zitierten Stand der Technik sind hier ein erstes Betriebssystem 351 sowie ein zweites Betriebssystem 352 im ROM Speicherbereich 33 eingebracht.

Zur Ausführung des Betriebssystems 35 ist im Sicherheitsmodul 3 eine zentrale Recheneinheit 32 als weitere Systemressource vorgesehen. Sie hat direkten Zugriff sowohl auf die Datenschnittstelle 31 als auch den Speicherbereich 33.

In Figur 2 ist die schichtenorientierte Softwarestruktur eines Sicherheitsmoduls 3 dargestellt. Dabei stellt die unterste Schicht, die Hardwareschicht 34 dar. Auf diese Hardwareschicht 34 greift das Betriebssystem 35 über Speicheradressverlinkungen direkt zu. In einigen Fällen kann zwischen Hardwareschicht 34 und Betriebssystem 35 noch eine Hardwareabstraktionsschicht (HAL) eingebracht werden (nicht dargestellt), die wie eingangs erwähnt nicht mit der erfindungsgemäßen Betriebssystemschnittstelle 36 zu verwechseln ist.

In dem Sicherheitsmodul 3 ist eine Primäranwendung 37 eingebracht, hier in Form einer Java Card virtuellen Maschine (JCVM) 371. Die JCVM wiederum stellt eine Laufzeitumgebung JCRE 373 zur Verfügung. Hier als Teil der Primäranwendung 37 gezeichnet, werden auch Programmcodebibliotheken 374 als Teil der Primäranwendung 37 gezeigt. Alternativ zu einer JCVM 371 als Primäranwendung wird ein nativer Dienst 372 als eine Primäranwendung 37

in das Sicherheitsmodul 3 eingebracht. Diese Primäranwendungen 37 greifen über Speicheradressverweise 41 - gemäß dem Stand der Technik - direkt auf das Betriebssystem 35 zu, hier durch die Pfeile 41 dargestellt.

Das Sicherheitsmodul 3 weist darüber hinaus Sekundäranwendungen 38 auf, welche auf die Primäranwendungen 37 zugreifen. Die Sekundäranwendungen 38 greifen nicht auf das Betriebssystem 35 zu, wodurch die Sekundäranwendungen 38 sehr abstrakt gehalten werden können. Als Sekundäranwendungen 38 sind hier beispielhaft Java-Applikationen 381 bzw. ein Dateisystem 384 dargestellt, die gemäß Speicheradressverweisen 40 auf die jeweilige Primäranwendung 37 zugreifen.

In Figur 3 ist eine vereinfachte Darstellung eines Speicherbereichs 33 eines erfindungsgemäßen Sicherheitsmoduls 3 gezeigt. Dabei ist erneut der Zusammenhang zwischen Sekundäranwendung 38 und Primäranwendung 37 gemäß Figur 2 dargestellt. Mittels Speicheradressverweisen 40 greift eine Sekundäranwendung 38 auf die Primäranwendung 37 zu. Erfindungsgemäß greift die Primäranwendung 37 nun nicht direkt auf das Betriebssystem 35 zu, sondern die Primäranwendung 37 greift auf eine Betriebssystemschnittstelle 36 mittels Speicheradressverweisen 41 zu. Nur die Betriebssystemschnittstelle 36 greift auf das aktivierte Betriebssystem 35 zu. Die Betriebssystemschnittstelle 36 greift mittels einer Speicheradresstabelle 42 auf das erste Betriebssystem 351 zu. Bei der dargestellten bevorzugten Ausführungsform weist die Betriebssystemschnittstelle 36 weiterhin bereits Speicheradressverweise 42 zum zweiten Betriebssystem 352 auf, sodass in diesem gezeigten Fall bereits eine Umsetzung vom ersten Betriebssystem 351 auf das zweite Betriebssystem 352 möglich ist.

Weiterhin dargestellt sind ein Bootloader 4 sowie ein Freispeicher 39, auch als Java-Heap bezeichnet.

Das zweite Betriebssystem 352 ist dabei mittels der Ladeeinheit 4 in einen reservierten Teil des Speichers 33 des Sicherheitsmoduls 3 während des Betriebs des Sicherheitsmoduls 3 nachgeladen worden. Dabei wurde eine Checksumme überprüft, um Manipulationen an dem zweiten Betriebssystem 352 ausschließen zu können.

Beispielsweise umfasst das zweite Betriebssystem 352 einen alternativen Funktionsumfang, einen alternativen Befehlssatz, einen verbesserten Kommandointerpreter im Vergleich zum ersten Betriebssystem 351. Beispielsweise ist die Version des ersten Betriebsystems 351 veraltet, sodass es durch eine neuere Version 352 zu ersetzen ist. Alternativ ist das zweite Betriebssystem lediglich eine alternative Variante, mit geänderten Funktionsumfängen, einer alternativen Dateiverwaltung oder dergleichen, um dem Sicherheitsmodul alternative Funktionen zu ermöglichen.

In Figur 4 ist eine Verlinkungstabelle 42, die von der Betriebssystemschnittstelle 36 verwendet wird, näher dargestellt. Rein exemplarisch sind die Links für die Betriebssystemkommandos 44 „write", „read" und „open" dargestellt. Alle, vom Betriebssystem 35 empfangenen Kommandos der Primäranwendung 37 werden in dieser Tabelle 42 in physikalische Speicheradressen aufgelöst.

Zu erkennen ist, dass für das erste Betriebssystem 351 andere Adressverweise 42 gelten als für das zweite Betriebssystem 352, da das zweite Betriebssystem 352 und alle entsprechenden Inhalte in anderen Teilen des Speicherbereichs 33 abgelegt sind als die Inhalte des ersten Betriebssystems 351. Die

Betriebssystemschnittstelle 36 analysiert daher die Primäranwendung 37 bezüglich Adressverweisen 41 auf das erste Betriebssystem 351 und ersetzt diese beim Umsetzen bzw. Umschalten auf das zweite Betriebssystem 352 gemäß der Verlinkungstabelle 42. Das Umsetzen kann auf einmal auf Basis eines Umsetzkommandos 6 erfolgen, sodass das Sicherheitsmodul in wenigen Taktzyklen mit dem zweiten Betriebssystem 352 wieder betriebsfähig ist.

In Figur 5 ist eine Darstellung der schichtenorientierten Softwarestruktur eines erfindungsgemäßen Sicherheitsmoduls mit zwei Betriebssystemen und einer Betriebssystemschnittstelle dargestellt. Die Hardwareschicht 34 als unterste Schicht wird von der Betriebssystemschicht 35 betrieben. Dabei sind hier erfindungsgemäß ein erstes Betriebssystem 351 und ein zweites Betriebssystem 352 dargestellt. Ein Umsetzer 5 dient zum Umsetzen des Sicherheitsmoduls 3 vom ersten Betriebssystem 351 auf das zweite Betriebssystem 352. Dazu wird beispielsweise das in Figur 3 und 4 beschriebene Verfahren der Verlinkungstabelle 42 angewendet. Oberhalb der Betriebssystemebene 35 ist die Betriebssystemschnittstelle 36 eingebracht, die die Schnittstelle zwischen den Primäranwendungen 37 und dem jeweiligen Betriebssystem 35 bildet. Als Primäranwendung 37 ist bspw. eine JCVM 371 mit JCRE 373 und API's 374 vorgesehen. Alternativ oder zusätzlich ist als Primäranwendung 37 ein nativer Dienst vorgesehen. Als Sekundäranwendungen 38 sind Applets 381, beispielsweise Bezahlapplikation, Authentisierungsapplikation, Teilnehmeridentitätsdatenumschaltungsapplikation (SMC) vorgesehen. Weiterhin können eine Sicherheitszone 383 oder ein Dateisystem 384 im Sicherheitsmodul 3 vorgesehen sein. Weiterhin können Teilnehmeridentitätsdaten 382 vorgesehen sein. Teilnehmeridentitätsdaten 382 sind zum einen Daten, die einen Teilnehmer eindeutig in einem Kommunikationsnetz (beispielsweise in einem Mobilfunknetz) identifizieren, beispielsweise eine International Mobile Subscriber Identity (IMSI) und/oder teilnehmerspezifische Da-

ten. Zum Anderen können die Teilnehmeridentitätsdaten Daten sein, die einen Teilnehmer eindeutig gegenüber dem Kommunikationsnetz authentisieren, beispielsweise ein Authentisierungsalgorithmus, spezifische Algorithmusparameter, ein kryptografischer Authentisierungsschlüssel oder ein kyptografischer Over-The-Air (OTA) Schlüssel.

In Figur 6 ist ein Ablaufdiagramm des erfindungsgemäßen Verfahrens zum Aktivieren eines Betriebssystems 35 in dem Sicherheitsmodul 3 dargestellt. Dabei steht das Sicherheitsmodul 3 über ein Endgerät 1 in Kommunikation mit einer entfernten Instanz 2. Während des Betriebs des Sicherheitsmoduls 3 im ersten Betriebssystem 351 informiert die entfernte Instanz 2, insbesondere ein Mobilfunkserver, über eine aktuellere Version des Betriebssystems 35 auf dem Sicherheitsmodul 3, im Folgenden als zweites Betriebssystem 352 bezeichnet. Das Sicherheitsmodul 3 oder das Endgerät 1 fordert das zweite Betriebssystem 352 von der entfernten Instanz 2 an. Dazu wird ein sicherer Kanal unter Authentisierung/Identifizierung des Sicherheitsmoduls 3 aufgebaut. Der Kanal ist bevorzugt ein Kommunikationskanal zwischen dem Endgerät 1 und dem Server 2, beispielsweise ein gemäß Bearer Independent Protocol, kurz BIP ausgebildeter Kommunikationskanal über ein Mobilfunknetz oder ein SMS Kanal gemäß GSM Spezifikation GSM 11.48. Alternative Kommunikationskanäle, beispielsweise WLAN, NFC sind ebenfalls möglich. Die Kommunikation kann over-the-air oder over-the-internet oder durch direkte Verbindung zu einem Terminal aufgebaut sein.

Der Server 2 stellt nach erfolgreicher Authentisierung des Endgeräts 1 bzw. des Sicherheitsmoduls 3 das zweite Betriebssystem 352 in verschlüsselter Form mit einer Checksumme zur Plausibilitätsprüfung zum Download bereit. Das Sicherheitsmodul lädt das zweite Betriebssystem 352 in den Speicherbereich 33, prüft die Plausibilität anhand der Checksumme, entschlüsselt

das zweite Betriebssystem und analysiert es bezüglich der Adressverlinkungen 41. Anschließend wird es durch das Umschaltkommando 6 aktiviert. Die Umschaltung kann insbesondere durch den Server 2 initiiert werden, beispielsweise mittels eines Umsetzkommandos 6. Nach einem Neustart des Sicherheitsmoduls 3 wird ein Funktionstest durchgeführt, wobei bei erfolgreichem Bestehen eine Bestätigungsinformation an die entfernte Instanz 2 gesendet wird. Anschließend wird das erste Betriebssystem 351 aus dem Speicherbereich gelöscht.

In einer nicht figürlich dargestellten Ausführung ist die JCVM 371 mit JCRE 372 ein Teil des Betriebssystems 35. In dieser Ausführung wird die JCVM 371 in der Ebene des Betriebssystems 35 geführt und ist Teil des ersten Betriebssystems 351. Das zweite Betriebssystem 352 weist dann ebenfalls eine JCVM 371 mit JCRE 373 auf. Die API's 374 sowie die Sekundäranwendungen 38 verbleiben beim Umsetzen 6 auf das zweite Betriebssystem 352 unverändert im Sicherheitsmodul 3. Die Betriebssystemschnittstelle 36 abstrahiert das Betriebssystem 35 und setzt auch die entsprechenden Verlinkungen bezüglich der virtuellen Maschine um. Die JCVM 371 ist in diesem Fall keine Primäranwendung 37.

Patentansprüche

1. Verfahren zum Aktivieren eines Betriebssystems (35) in einem Sicherheitsmodul (3), wobei das Sicherheitsmodul (3) entweder mittels eines ersten Betriebssystems (351) oder mittels eines zweiten Betriebssystems (352) betriebsfähig ist, mit den Verfahrensschritten:

- Betreiben des Sicherheitsmoduls (3) mittels des ersten Betriebssystems (351) und
- Umsetzen (6) des Sicherheitsmoduls (3) vom ersten Betriebssystem (351) auf das zweite Betriebssystem (352);

dadurch gekennzeichnet, dass:

- eine in das Sicherheitsmodul (3) eingebrachte Primäranwendung (37) mittels einer Betriebssystemschnittstelle (36) auf das jeweilige Betriebssystem (35) zugreift, sodass die eingebrachte Primäranwendung (37) durch den Schritt des Umsetzens (6) unverändert bleiben kann.

2. Verfahren nach Anspruch 1, wobei:

- die eingebrachte Primäranwendung (37) nur über die Betriebssystemschnittstelle (36) auf das erste Betriebssystem (351) oder das zweite Betriebssystem (352) zugreift; und
- die Primäranwendung (37) zur Ausführung mindestens einer Sekundäranwendung (38) eingerichtet ist, wobei die Sekundäranwendung (38) nur mittels der Primäranwendung (37) und der Betriebssystemschnittstelle (36) auf das erste Betriebssystem (351) oder das zweite Betriebssystem (352) zugreifen kann.

3. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Primäranwendung (37) eine virtuelle Maschine (371) und/oder ein nativer Dienst (372) ist.

4. Verfahren nach einem der Ansprüche 1 oder 2, wobei eine virtuelle Maschine (371) Teil des ersten Betriebssystems (351) sowie des zweiten Betriebssystems (352) ist.

5. Verfahren nach einem der vorhergehenden Ansprüche, wobei das Aktivieren des zweiten Betriebssystems (352) durch Umsetzen (6) von Speicheradressverweisen (41) in der Betriebssystemschnittstelle (36) realisiert wird.

6. Verfahren nach einem der vorhergehenden Ansprüche, wobei das zweite Betriebssystem (352) vor dem Schritt des Umsetzens (6) in einen Speicherbereich (33) des Sicherheitsmoduls (3) geladen wird.

7. Verfahren nach einem der vorhergehenden Ansprüche, wobei vor dem Schritt des Umsetzens (6) die Betriebssystemschnittstelle (36) das erste Betriebssystem (351) auf Speicheradressverweise (41) zwischen der Primäranwendung (37) und dem ersten Betriebssystem (351) analysiert und diese Speicheradressverweise (41) in einer Speicheradresstabelle (42) ablegt.

8. Verfahren nach einem der vorhergehenden Ansprüche, wobei das zweite Betriebssystem (352) vor dem Schritt des Umsetzens (6) in einen Speicherbereich (33) des Sicherheitsmoduls (3) in verschlüsselter Form geladen wird und auf Plausibilität geprüft wird.

9. Verfahren nach einem der vorhergehenden Ansprüche, wobei nach dem Schritt des Umsetzens (6) eine Bestätigungsinformation an eine entfernte Instanz (2) gesendet wird.

10. Verfahren nach einem der vorhergehenden Ansprüche, wobei das erste Betriebssystem (351) nach dem Schritt des Umsetzens (6) auf das zweite Betriebsystem (352) gelöscht wird.

11. Sicherheitsmodul (3) mit einer zentralen Recheneinheit (32), einem Speicherbereich (33) und einer Datenschnittstelle (31), wobei im Speicherbereich (33) ein erstes Betriebssystem (351) und zumindest eine Primäranwendung (37) abgelegt ist, wobei das Sicherheitsmodul (3) mit dem ersten Betriebssystem (351) betriebsfähig ist;
dadurch gekennzeichnet, dass:
- das Sicherheitsmodul (3) eine Betriebssystemschnittstelle (36) mit direktem Zugriff auf das erste Betriebssystem (351) aufweist; und
- die Primäranwendung (37) indirekt über die Betriebssystemschnittstelle (36) auf das erste Betriebssystem (351) zugreift.

12. Sicherheitsmodul (3) nach Anspruch 11, wobei:
- im Speicherbereich (33) ein zweites Betriebssystem (352) abgelegt ist;
- die Betriebssystemschnittstelle (36) direkt auf das zweite Betriebssystem (352) zugreift; und
- das Sicherheitsmodul (3) einen Umsetzer (5) zum Umsetzen zwischen dem ersten Betriebssystem (351) und dem zweiten Betriebssystem (352) aufweist, wobei die Primäranwendung (37) unverändert bleibt.

13. Sicherheitsmodul (3) nach einem der Ansprüche 10 bis 12, wobei das zweite Betriebssystem (352) über die Datenschnittstelle (31) in den Speicherbereich (33) ladbar ist.

14. Sicherheitsmodul (3) nach einem der Ansprüche 10 bis 13, wobei eine Ladeeinheit (4) im Sicherheitsmodul (3) zum Laden des zweiten Betriebssystems (352) vorgesehen ist.

15. Verwenden eines Sicherheitsmoduls (3) gemäß den Ansprüchen 10 bis 14 in einem Endgerät (1), wobei das zweite Betriebssystem (352) von einer entfernten Instanz (2) über ein mobiles Kommunikationsnetz bereitgestellt wird.

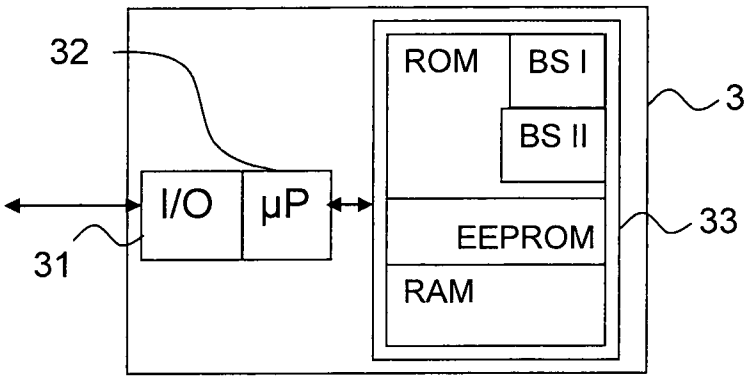

Fig. 1 – Stand der Technik

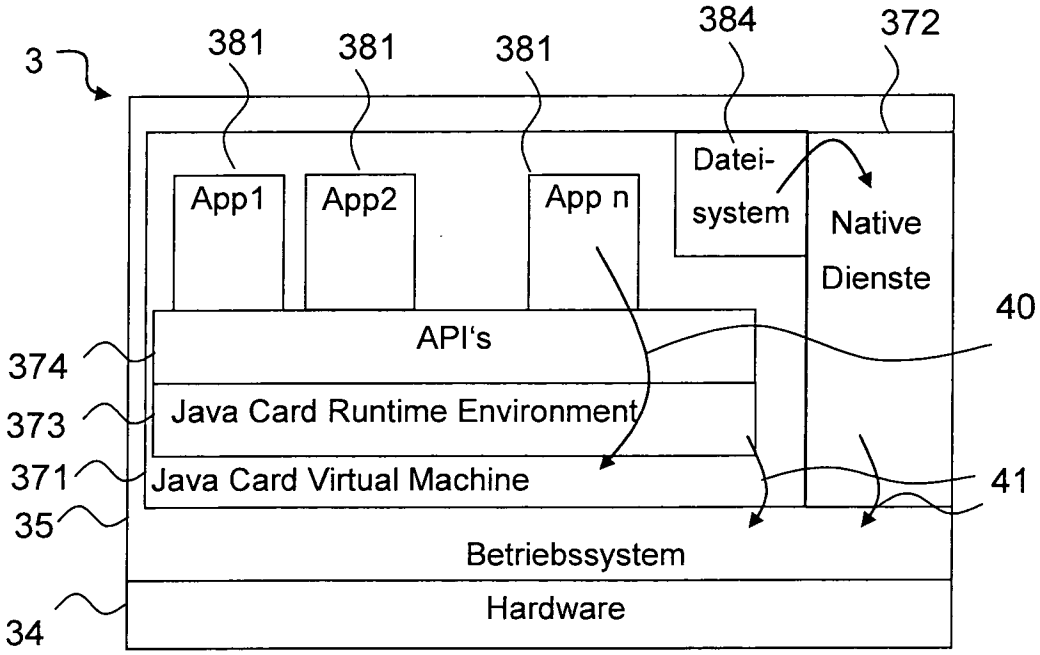

Fig. 2

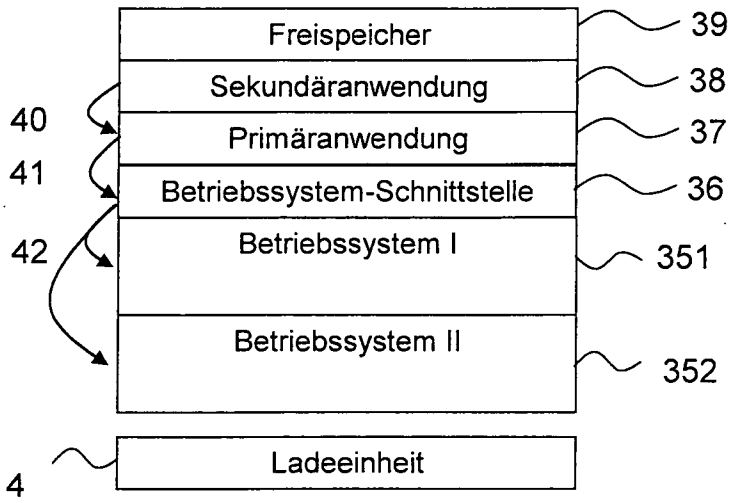
Freispeicher
Sekundäranwendung
Primäranwendung
Betriebssystem-Schnittstelle
Betriebssystem I
Betriebssystem II
Ladeeinheit
39
38
37
36
351
352
4
40
41
42

Fig. 3

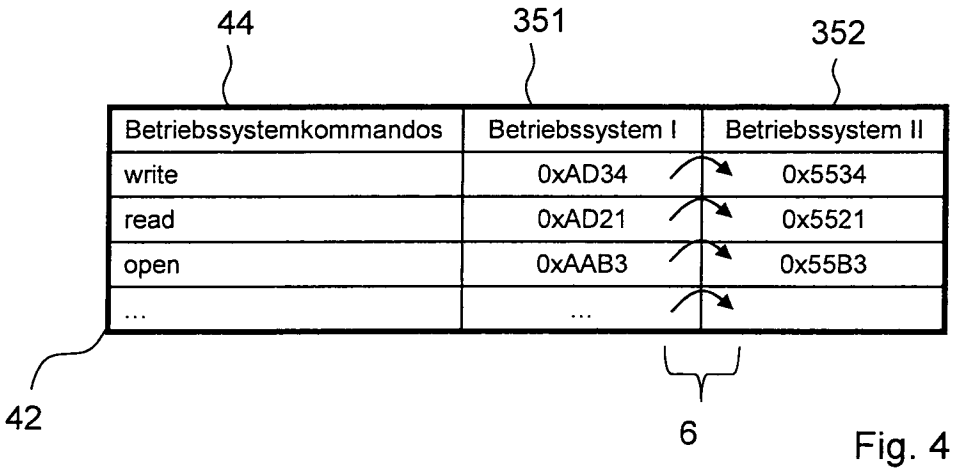
44
351
352
Betriebssystemkommandos
Betriebssystem I
Betriebssystem II
write
0xAD34
0x5534
read
0xAD21
0x5521
open
0xAAB3
0x55B3
...
...
42
6

Fig. 4

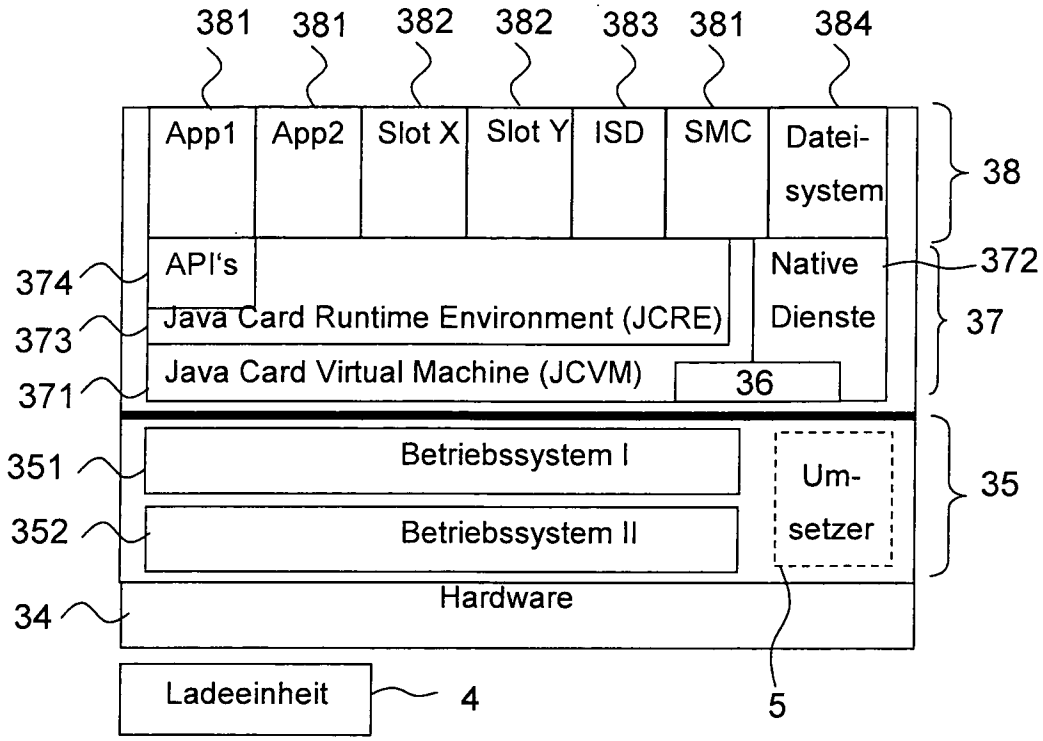
381
381
382
382
383
381
384
App1
App2
Slot X
Slot Y
ISD
SMC
Datei-system
38
API's
Native
Dienste
372
37
374
373
371
Java Card Runtime Environment (JCRE)
Java Card Virtual Machine (JCVM)
36
351
352
Betriebssystem I
Betriebssystem II
Um-setzer
35
34
Hardware
Ladeeinheit
4
5

Fig. 5

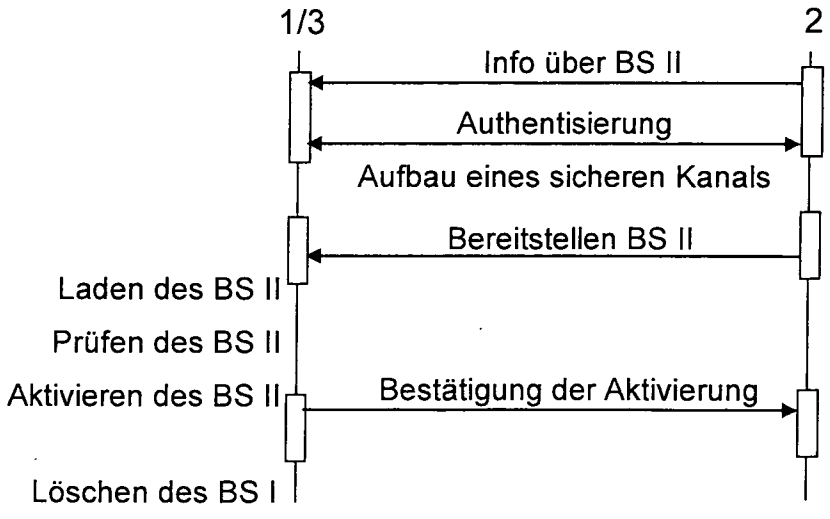
1/3
2
Info über BS II
Authentisierung
Aufbau eines sicheren Kanals
Bereitstellen BS II
Laden des BS II
Prüfen des BS II
Aktivieren des BS II
Bestätigung der Aktivierung
Löschen des BS I

Fig. 6

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2013/002152

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F9/445
ADD.

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)
G06F

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 practicable, 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	US 2012/110274 A1 (ROSALES JACOB J [US] ET AL ROSALES JACOB JASON [US] ET AL) 3 May 2012 (2012-05-03) paragraph [0005] - paragraph [0006] paragraph [0082] - paragraph [0098] -----	1-15
A	US 6 154 878 A (SABOFF MICHAEL L [US]) 28 November 2000 (2000-11-28) the whole document -----	1-15

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

☒ See patent family 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 application or patent 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
20 September 2013	30/09/2013

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, Fax: (+31-70) 340-3016	Bijn, Koen

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2013/002152

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2012110274 A1	03-05-2012	NONE	
US 6154878 A	28-11-2000	NONE	

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2013/002152

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. G06F9/445
ADD.

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
G06F

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	US 2012/110274 A1 (ROSALES JACOB J [US] ET AL ROSALES JACOB JASON [US] ET AL) 3. Mai 2012 (2012-05-03) Absatz [0005] - Absatz [0006] Absatz [0082] - Absatz [0098] -----	1-15
A	US 6 154 878 A (SABOFF MICHAEL L [US]) 28. November 2000 (2000-11-28) das ganze Dokument -----	1-15

☐ 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" frühere Anmeldung oder Patent, die bzw. 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 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
20. September 2013	30/09/2013

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Bijn, Koen

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2013/002152

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2012110274 A1	03-05-2012	KEINE	
US 6154878 A	28-11-2000	KEINE	