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

(10) **DE 697 20 614 T2** 2004.02.12

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 0 821 508 B1**
(21) Deutsches Aktenzeichen: **697 20 614.9**
(96) Europäisches Aktenzeichen: **97 110 865.9**
(96) Europäischer Anmeldetag: **01.07.1997**
(97) Erstveröffentlichung durch das EPA: **28.01.1998**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **09.04.2003**
(47) Veröffentlichungstag im Patentblatt: **12.02.2004**

(51) Int Cl.[7]: **G06F 1/00**
H04L 9/32, H04L 29/06

(30) Unionspriorität:
685076 **23.07.1996** **US**

(84) Benannte Vertragsstaaten:
DE, FR, GB

(73) Patentinhaber:
Cheyenne Property Trust, San Francisco, Calif., US

(74) Vertreter:
Schoppe, Zimmermann, Stöckeler & Zinkler, 82049 Pullach

(72) Erfinder:
Klemba, Keith, Palo Alto, US; Merkling, Roger, Palo Alto, US

(54) Bezeichnung: **Verschlüsselungseinheit mit Kontaktpunktlogik**

Beschreibung

Hintergrund der Erfindung Technisches Gebiet

[0001] Die Erfindung bezieht sich auf Kryptographie. Insbesondere bezieht sich die Erfindung auf eine kryptographische Einheit für die Verwendung mit einer internationalen Kryptographiegrundstruktur.

Beschreibung des Stands der Technik

[0002] Kunden von großen Computersystemen sind typischerweise multinationale Konzerne, die firmenweite computerbasierte Lösungen kaufen möchten. Die verteilte Natur solcher Organisationen erfordert es, daß dieselben öffentliche internationale Kommunikationsdienste verwenden, um Daten innerhalb ihrer Organisation zu transportieren. Selbstverständlich sind sie besorgt um die Sicherheit ihrer Kommunikation und möchten moderne Ende-zu-Ende-Kryptographiemöglichkeiten verwenden, um Geheimhaltung und Datenintegrität sicherzustellen.

[0003] Die Verwendung von Kryptographie in der Kommunikation wird durch nationale Richtlinien bzw. Taktik (Policy) bestimmt und leider unterscheiden sich die nationalen Richtlinien bezüglich dieser Verwendung. Jede nationale Richtlinie wird unabhängig entwickelt, im allgemeinen mit einem nationaleren Schwerpunkt anstatt internationalen Überlegungen. Es gibt Standardgruppen, die versuchen, einen gemeinsamen kryptographischen Algorithmus zu entwickeln, der für eine internationale Kryptographie geeignet ist. Das Thema der internationalen Kryptographiestandards ist jedoch kein technisches Problem, sondern ein politisches Thema, dem die nationale Souveränität zugrunde liegt. Als solches ist es unrealistisch zu erwarten, daß die unterschiedlichen nationalen Kryptographierichtlinien durch einen technischen Standardisierungsprozeß aufeinander abgestimmt werden.

[0004] Das Thema nationaler Interessen bei der Kryptographie ist von besonderem Belang für Firmen, die Informationstechnologieprodukte auf der Basis eines offenen Standards für einen weltweiten Markt herstellen. Der Markt erwartet, daß diese Produkte sicher sind. Immer mehr Verbraucher dieser Produkte sind jedoch selbst multinational und fordern von den Herstellern, daß sie ihnen dabei helfen, die internationalen Kryptographieprobleme zu lösen, die ihre weltweite Informationstechnologieentwicklung hemmen. Die anhaltenden ungelösten Unterschiede und Exportbeschränkungen bei nationalen Kryptographierichtlinien haben einen nachteiligen Effekt auf das Wachstum des internationalen Marktes für sichere offene Rechenprodukte. Somit wäre es hilfreich, eine internationale Grundstruktur zu schaffen, die globale Informationstechnologieprodukte liefert, die gemeinsame Sicherheitselemente aufweisen, während sie gleichzeitig die unabhängige Entwicklung nationaler Kryptographierichtlinien respektieren.

[0005] Die Nationen haben Gründe zum Einführen von Richtlinien, die die Kryptographie regeln. Häufig haben diese Gründe mit dem Vollzug von Gesetzen und nationalen Sicherheitsthemen zu tun. Innerhalb jedes Landes kann es zwischen der Regierung und dem Volk Debatten über die Richtigkeit und Annehmbarkeit dieser Richtlinien geben. Anstatt sich an diesen Debatten zu beteiligen oder zu versuchen, deren Ergebnis vorherzusagen, ist es praktischer, das souveräne Recht jeder Nation, eine unabhängige Richtlinie festzulegen, die die Kryptographie in der Kommunikation regelt, zu akzeptieren.

[0006] Richtlinien, die die nationale Kryptographie regeln, drücken nicht nur den Willen des Volkes und der Regierung aus, sondern umfassen auch bestimmte Technologien, die Kryptographie ermöglichen. Die Wahl der Technologie ist sicherlich ein Bereich, wo die Standardisierung eine Rolle spielen kann. Wie es früher angemerkt wurde, ist dies jedoch nicht lediglich ein technisches Problem, so daß zum Beispiel die Auswahl gemeinsamer kryptographischer Technologien allein die Unterschiede bei den nationalen Richtlinien nicht lösen kann. Folglich wäre es nützlich, eine gemeinsame akzeptierte Kryptographiegrundstruktur zu schaffen, bei der unabhängige Technologie und Richtlinienauswahlen auf eine Weise getroffen werden können, die nach wie vor eine internationale Kryptographiekommunikation ermöglicht, die mit diesen Richtlinien übereinstimmt.

[0007] Eine Vier-Teil-Technologiegrundstruktur, die eine internationale Kryptographie unterstützt, die eine nationale Flagkarte, eine kryptographische Einheit, ein Hostsystem und einen Netzwerksicherheitsserver umfaßt, ist offenbart in K. Klemba, R. Merckling, International Crytpography Framework in einer mitanhängigen U.S.-Patentanmeldung mit der Seriennummer 08/401,588, die am 8. März 1995 eingereicht wurde. Drei dieser vier Dienstelemente haben eine im wesentlichen hierarchische Beziehung. Die nationale Flagkarte (NFC = National Flag Card) ist in der kryptographischen Einheit (CU = Cryptographic Unit) installiert, die wiederum in einem Hostsystem (HS) installiert ist. Kryptographische Funktionen auf dem Hostsystem können nicht ohne eine kryptographische Einheit ausgeführt werden, die selbst das Vorliegen einer gültigen nationalen Flagkarte erfordert, bevor die Dienste derselben verfügbar sind. Das vierte Dienstelement, ein Netzwerksicherheitsserver (NSS = Network Security Server), kann einen Bereich von unterschiedlichen Sicherheitsdiensten liefern, einschließlich der Verifizierung der anderen drei Dienstelemente.

[0008] Die Grundstruktur unterstützt den Entwurf, die Implementierung und Betriebselemente jeder und aller nationalen Richtlinien, während der Entwurf, die Entwicklung und der Betrieb der unabhängigen Sicherheitsrichtlinien vereinheitlicht wird. Die Grundstruktur gibt daher den Dienstelementen der nationalen Sicherheitsrichtlinien eine Standardform, wo solche Dienstelemente Dinge wie Hardwareformfakto-

ren, Kommunikationsprotokolle und Online- und Offline-Datendefinitionen umfassen.

[0009] Kritisch für die Implementierung der Grundstruktur ist die Bereitstellung einer grundlegenden Technologie, die die Herstellung der verschiedenen Dienstelemente ermöglicht. Obwohl verschiedene Implementationen der Dienstelemente innerhalb der Fähigkeiten eines Fachmanns auf diesem Gebiet liegen, gibt es einen Bedarf an spezifischen Verbesserungen des Stands der Technik, falls das volle Potential der Grundstruktur realisiert werden soll.

[0010] Die WO 95/14338 bezieht sich auf ein Computersystem zum Lesen verschlüsselter Informationen. Eine Entschlüsselungseinheit ist vorgesehen, die in der Lage ist, nur von einen verschlossenen zu einen offenen Zustand überzugehen, wenn dieselbe zusätzlich zu einem vorbestimmten externen Schlüssel ein vorbestimmtes Aktivierungssignal empfängt. Ein Anzeigetool emittiert das vorbestimmte Aktivierungssignal zu der Entschlüsselungseinheit, wenn dieselbe in einem Systemmodalbetriebsmodus ist. Der vorbestimmte externe Schlüssel ist ein Barcode, der beispielsweise durch einen Stiftleser erfaßt werden kann. Das vorbestimmte Aktivierungssignal besteht aus einer eindeutigen Bitsequenz, die durch das Anzeigetool wiederholt in festen Intervallen erzeugt wird. Eine Überwachungseinrichtung ist vorgesehen, die die Entschlüsselungseinheit zwingt, in den verschlossenen Zustand überzugehen, falls die eindeutige Bitsequenz nicht innerhalb der festgelegten Intervalle wiederholt empfangen wird.

[0011] Verfahren zum Errichten und Geltendmachen einer kryptographischen Netzwerksicherheitsrichtlinie in einem Öffentlicher-Schlüssel-Kryptosystem sind in der US-5,164,988 offenbart.

[0012] D. Conner: „Reconfigurable Logic", EDN electrical design news, Bd. 41, Nr. 7, 28. März 1996, S. 53 bis 56, 58, 60 und 62 bis 64 beschreibt die Möglichkeiten und Vorteile einer rekonfigurierbaren Logik.

[0013] Verfahren und Vorrichtungen für den Schutz und die Steuerung von Computerprogrammen sind in der US-A-4,649,510 offenbart.

[0014] In R. Ferreira: „The Practical Application of State of the Art Security in Real Environments", Advances in Cryptology AUSCRYPT '90, 8 . Januar 1990, S . 334 bis 355 wird die Anwendung von herkömmlicher Sicherheit in echten Umgebungen, die Smart Cards verwenden, gelehrt.

[0015] Schließlich beschreibt T. Y. C. Woo u. a. „Authentication for Distributed Systems", Computer, Bd. 25, Nr. 1, 1. Januar 1992, S. 39 bis 52 Sicherheitsaspekte in verteilten Systemen über Authentifizierungslösungsansätze unter Verwendung von Smart Cards.

[0016] Es ist die Aufgabe der vorliegenden Erfindung, eine kryptographische Einheit und ein Verfahren zum Verhindern einer unbefugten Verwendung von kryptographischen Funktionen zu schaffen, die es ermöglicht, daß das gesamte Potential internationaler Kryptographiegrundstrukturen realisiert wird.

[0017] Diese Aufgabe wird durch eine kryptographische Einheit gemäß Anspruch 1 und ein Verfahren gemäß Anspruch 21 gelöst.

[0018] Die internationale Kryptographiegrundstruktur ermöglicht es Herstellern, verschiedene nationale Gesetze zu erfüllen, die die Verteilung kryptographischer Fähigkeiten bestimmen.

[0019] Insbesondere macht es eine solche Grundstruktur möglich, weltweite kryptographische Fähigkeiten in allen Typen von Informationsverarbeitungsgeräten (z. B. Druckern, Palmtops) zu versenden. Innerhalb der Grundstruktur enthält eine kryptographische Einheit mehrere kryptographische Verfahren (z. B. DES, RSA, MD5). Diese Verfahren werden auf vorbestimmte Weisen an mehreren Punkten deaktiviert, die als Berührungspunkte (TP = Touch Points) bezeichnet werden.

[0020] An jedem TP gibt es eine dynamische Zustandsfreigabelogik, die ein sogenanntes Berührungspunktgatter (TPG = Touch Point Gate) bildet. TPGs erfordern eine regelmäßige Neukonfiguration um den TP in dem freigegebenen Zustand zu halten. Einem TP können auch Beschränkungsdaten zugeordnet sein. Diese Beschränkungsdaten werden als Berührungspunktdaten (TPD = Touch Point Data) bezeichnet und liefern eine parametrische Steuerung der Funktionsweise des Verfahrens.

[0021] Jedes kryptographische Verfahren wird durch mehrere TPs in diesem Verfahren gesteuert. Alle TPGs für ein bestimmtes kryptographisches Verfahren müssen in einem freigegebenen Zustand sein, um dieses Verfahren freizugeben. Weil der Freigabezustand jedes TPG dynamisch ist, ist eine konstante Auffrisch- und Zustandsbestimmung erforderlich. Diese Auffrischung wird erreicht durch einen sogenannten Berührungspunktherzschlag (TPH = Touch Point Heartbeat) erreicht, der zwischen der CU und dem nationalen Flagkarte- (die auch als eine Richtlinienkarte bezeichnet wird), Dienstelement der internationalen Kryptographiegrundstruktur. Alle Aspekte der Berührungspunkte zusammen werden als Berührungspunktlogik (TPL = Touch Point Logic) bezeichnet.

Kurze Beschreibung der Zeichnungen

[0022] **Fig.** 1 ist ein Blockdiagramm einer internationalen Kryptographiegrundstruktur, die eine nationale Flagkarte, eine kryptographische Einheit, ein Hostsystem und einen Netzwerksicherheitsserver umfaßt;

[0023] **Fig.** 2 ist eine schematische Darstellung, die ein allgemeines Berührungspunktprinzip gemäß der Erfindung zeigt;

[0024] **Fig.** 3 ist eine schematische Darstellung, die einen spezifischen Berührungspunkt zeigt, der eine Signaturerzeugung gemäß der Erfindung liefert;

[0025] **Fig.** 4 ist ein Zeitgebungsdiagramm, das das Verhalten einer kryptographischen Einheit während einer Aktivierungsstufe gemäß der Erfindung zeigt;

[0026] **Fig.** 5 ist eine schematische Darstellung, die eine Dienstklasseninstallation gemäß der Erfindung

zeigt;

[0027] **Fig.** 6 ist eine schematische Darstellung, die eine Sicherheitsdomainautorität, Anwendungsdomainautorität und Anwendungsverschachtelung gemäß der Erfindung zeigt;

[0028] **Fig.** 7 ist eine schematische Darstellung, die einen Berührungspunktdatenlebenszyklus einschließlich der Erzeugung, Installation/Verteilung und des Ladens gemäß der Erfindung zeigt;

[0029] **Fig.** 8 ist ein Zeitgebungsdiagramm, das das Verhalten einer kryptographischen Einheit während einer Betriebsstufe gemäß der Erfindung zeigt;

[0030] **Fig.** 9 ist eine schematische Darstellung, die einen Berührungspunktdatenlebenszyklus einschließlich einer Aktualisierung gemäß der Erfindung zeigt;

[0031] **Fig.** 10 ist eine schematische Darstellung, die die Funktionselemente einer Kryptographischen Einheit gemäß der Erfindung zeigt;

[0032] **Fig.** 11 ist eine schematische Darstellung, die eine Ladesequenz gemäß der Erfindung zeigt;

[0033] **Fig.** 12 ist eine schematische Darstellung, die einen Fluß von Ereignissen für eine Berührungspunktdatenladesequenz gemäß der Erfindung zeigt; und

[0034] **Fig.** 13 ist eine schematische Darstellung, die einen Fluß von Ereignissen für eine Anwendung a1 zeigt, die eine kryptographische Funktion 1 gemäß der Erfindung zeigt.

Detaillierte Beschreibung der Erfindung

[0035] Nationale Kryptographierichtlinien schwanken oft nach Industriesegment, politischem Klima und/oder Mittelungsfunktion. Dies macht es schwierig, eine einheitliche Richtlinie für alle Industrien für alle Zeiten zuzuweisen. Folglich ist die Flexibilität einer kryptographischen Grundstruktur, die eine nationale Flagkarte umfaßt, sehr attraktiv. Die Erfindung bezieht sich daher auf das Lösen von Problemen im Zusammenhang mit internationaler Kryptographie. Dieselbe präsentiert eine Kryptographieeinheit für eine Grundstruktur, die verwendet werden kann, um den Entwurf und die Entwicklung jeder nationalen Richtlinie bezüglich Kryptographie zu unterstützen. Somit implementiert die Erfindung eine „Pförtner"-Funktion, durch die sowohl die Verwendung von Kryptographie als auch die Verwendung eines Systems, das durch die Kryptographie geschützt wird, auf eine geschützte und eingriffssichere Weise gesteuert werden.

[0036] Die Kryptographieeinheit, die die Erfindung umfaßt, befindet sich vorzugsweise in einer internationalen Kryptographiegrundstruktur, die vier Dienstelemente aufweist, von denen jedes unterschiedliche Diensttypen liefert. **Fig.** 1 ist ein Blockdiagramm der internationalen Kryptographiegrundstruktur (ICF = international cryptography framework) 10, die eine nationale Flagkarte **12**, eine kryptographische Einheit **14**, ein Hostsystem **16** und einen Netzwerksicherheitsserver **18** umfaßt. Drei der vier Dienstelemente haben eine im wesentlichen hierarchische Beziehung. Die nationale Flagkarte (NFC) ist in der kryptographischen Einheit (CU) installiert, die wiederum in einem Hostsystem (HS) installiert ist. Kryptographische Funktionen auf dem Hostsystem können nicht ohne eine kryptographische Einheit ausgeführt werden, die selbst das Vorliegen einer gültigen nationalen Flagkarte erfordert, bevor die Dienste derselben verfügbar sind. Für die Zwecke der Erörterung wird die nationale Flagkarte hierin auch als die Taktikeinrichtung bezeichnet, weil dieselbe die Disziplin liefert, die eine nationale kryptographische Taktik bzw. Richtlinie ausübt.

[0037] Das vierte Dienstelement, ein Netzwerksicherheitsserver (NSS) liefert einen Bereich von unterschiedlichen Sicherheitsdiensten, einschließlich der Verifizierung der anderen drei Dienstelemente, und wirkt somit als ein vertrauenswürdiger Dritter. Mitteilungen, die unter Verwendung der vorgeschlagenen Grundstruktur verschlüsselt sind, tragen einen elektronischen Stempel, der die nationale Kryptographietaktik identifiziert, unter der die Mitteilung verschlüsselt wurde. Der Netzwerksicherheitsserver liefert auch Stempelverifizierungsdienste für Mitteilungshandhabungssysteme.

[0038] Die ICF ermöglicht es Herstellern, verschiedene nationale Gesetze zu erfüllen, die die Verteilung kryptographischer Fähigkeiten regeln. Insbesondere macht es eine solche Grundstruktur möglich, weltweite kryptographische Fähigkeiten in alle Typen von Informationsverarbeitungsgeräten (z. B. Drucker, Palmtops) zu versenden.

[0039] In der ICF enthält eine CU mehrere kryptographische Verfahren (z. B. DES, RSA, MD5). Diese Verfahren sind auf vorbestimmte Weisen an mehreren Punkten freigegeben, die als Berührungspunkte (TP) bezeichnet werden. An jedem TP gibt es eine dynamische Zustandsfreigabelogik, das sogenannte Berührungspunktgatter (TPG). TPGs erfordern eine regelmäßige Neukonfiguration, um den TP in einem freigegebenen Zustand zu halten. Einem TP können auch Beschränkungsdaten zugeordnet sein. Diese Beschränkungsdaten werden als Berührungspunktdaten (TPD) bezeichnet und liefern eine parametrische Steuerung über der Funktionsweise jedes TP.

[0040] Kritisch für die Erfindung ist die Bereitstellung einer Kryptographie, die absichtlich ruht und die ohne das Vorliegen einer Verknüpfung zu einer getrennten Taktikeinrichtung nicht gezwungen werden kann, zu arbeiten. Die Erfindung bezieht sich insbesondere auf die Art und Weise wie die Kryptographie ruht und wie dieselbe auf eine Weise neu zusammengesetzt wird, die die erforderliche Verknüpfung beibehält, so daß es nicht möglich ist, die Kryptographie zu beginnen, dann die Verknüpfung zu entfernen und die Kryptographie ohne eine solche Verknüpfung am laufen zu halten. Folglich umfaßt die Erfindung einen Herzschlag, der das Vorliegen einer solchen Verknüpfung zu allen Zeiten erfordert. Ferner muß die

kryptographische Einheit auf eine Weise implementiert sein, die erkennt, daß die Gesellschaft verlangt und die Geschäftswelt fordert, daß alle Aspekte der kryptographischen Einheit überwachbar sein müssen. Das heißt, es muß möglich sein, alles innerhalb der kryptographischen Einheit zu wissen und zu sehen. Diese Konzepte sind für die hierin offenbarte kryptographische Einheit grundlegend.

[0041] Ein Merkmal der Erfindung liefert unterschiedliche Taktikkarten, die die kryptographische Einheit auf unterschiedliche Weisen freigeben, so daß die kryptographische Einheit unterschiedliche Betriebsweisen haben kann. Die Merkmale der kryptographischen Einheit, die es dem System ermöglichen, eine neue Funktionalität beispielsweise von einem Netzwerksicherheitsserver herunterzuladen, müssen ermöglichen, daß nur eine ruhende Kryptographie, die nur in einer geeigneten Weise durch eine getrennte Taktikeinrichtung freigegeben werden kann, heruntergeladen werden kann.

[0042] Die Berührungspunkttechnologie ist derzeit in einem Gatterarray implementiert, das typischerweise mehrere Berührungspunkte für ein einziges kryptographisches Verfahren, z. B. DES, erlaubt. Für den Zweck der Erörterung hierin bezieht sich das Wort „Verfahren" auf einen kryptographischen Algorithmus, wie zum Beispiel DES und RSA.

[0043] Andere Ausführungsbeispiele der Erfindung ermöglichen es, daß Gatter von verschiedenen Verfahren gemischt werden, so daß mehrere Bits, die die verschiedenen Gatter darstellen, bezüglich der speziellen Struktur, die dieselben implementieren, unbekannt sind. Die Gatter können in einer Struktur gesetzt sein, die in dem Fall eines Sicherheitsverstoßes einen allmählichen Verfall der Funktionalität bewirken, anstatt alle der mehreren Gatter auf einmal zu unterbrechen. Alternativ kann ein Gatter unabhängig ausgewählt und zufällig freigegeben werden. Somit kann eine Struktur gewählt werden, um die Schwierigkeit des Erfassens und Vereitelns der Berührungspunktmethode weiter erhöhen. Somit ermöglicht die Erfindung die Kombination verschiedener Verfahren und Berührungspunkte, z. B. bis zu 100–200 Berührungspunkte, in einer kryptographischen Einheit, wo jede Kombination oder Auswahl dieser Berührungspunkte zu jedem Zeitpunkt freigegeben werden kann.

[0044] Der Herzschlag ist ein fortlaufendes Protokoll, das die Kryptographie freigibt. Durch die kryptographische Einheit wird regelmäßig eine Abfrage gesendet. Als Folge muß die Taktikeinrichtung vorliegen. Falls die Taktikeinrichtung besetzt ist oder nicht vorliegt, verfällt die Kryptographie allmählich, weil die Berührungspunkte beginnen, abzunehmen, weil dieselben nicht die Antworten empfangen, die sie benötigen, um freigegeben zu bleiben. Folglich hängt das gesamte System von der Taktikeinrichtung ab. Falls die Taktikeinrichtung entfernt wird, unabhängig davon, was sonst in dem System vorgeht, beginnt die Funktionalität der Hardware zusammenzubrechen.

[0045] Die Rate eines Herzschlags hängt von der Taktikeinrichtung ab und ist ein Teil der wesentlichen zusätzlichen Berührungspunktdaten, die durch die Taktikkarte geliefert werden. Die Berührungspunktdaten werden typischerweise nur einmal an die kryptographische Einheit geliefert. Wenn die kryptographische Einheit und die Taktikeinrichtung initialisiert werden, sendet die Taktikeinrichtung ihre Berührungspunktdaten einmal hinüber, weil sich diese Daten nicht ändern. Die Gatterlogik in der kryptographischen Einheit ändert sich jedoch immer.

[0046] Ein Teil der Berührungspunktdaten, die an die kryptographische Einheit gesendet werden, bestimmt die Frequenz, mit der die Taktikeinrichtung, von der kryptographische Einheit Abragen erwartet. Dieser Datenaustausch funktioniert in beide Richtungen. Falls die kryptographische Einheit beispielsweise keine Abfragen an die Taktik sendet, d. h. wenn die kryptographische Einheit einmal gestartet wird und danach keine weiteren Abfragen an die Taktikeinrichtung gesendet werden erfaßt die Taktikeinrichtung, daß sich die kryptographische Einheit nicht an die Regeln hält. Falls somit die Taktikeinrichtung die kryptographische Einheit angewiesen hat, jede Sekunde eine Antwort zu senden, aber dieselbe nicht jede Sekunde eine Antwort sendet, bricht die Taktikeinrichtung die kryptographische Funktion ab. Falls die kryptographische Einheit ferner jemals abgeschaltet wird, läßt es die Taktikeinrichtung nicht zu, daß dieselbe wieder eingeschaltet wird.

[0047] Die Taktikeinrichtung behält ihren Zustand bei, und falls es die kryptographische Einheit ablehnt, eine Taktikanforderung zu erfüllen, findet die Umkehrung statt. Wenn die Leistung zu der kryptographischen Einheit abgeschaltet ist erkennt die Taktik sie nicht mehr. Das Ein- und Ausschalten ist eine Initialisierungssequenz oder eine Aktivierungssequenz (wie es nachfolgend näher erörtert wird). Falls das System eingeschaltet ist und läuft, erzwingen die Taktikeinrichtung und die kryptographische Einheit in regelmäßigen Intervallen eine Aktivierungssequenz. Selbst wenn in die kryptographische Einheit eingegriffen wurde, so daß dieselbe als ein legitimes Systemelement erscheint, muß dieselbe an einem gewissen Punkt trotzdem eine Initialisierungsphase erfüllen, die eine Leistungsrücksetzung der kryptographischen Einheit ist, und es gibt keine Möglichkeit, daß die kryptographische Einheit diese Anforderung umgehen kann.

[0048] Das bevorzugte Ausführungsbeispiel der Erfindung plaziert die kryptographische Einheit in eine getrennte Hardwareeinheit von der der Taktikeinrichtung. Obwohl die kryptographische Funktion in Software anstatt in Hardware implementiert werden könnte, ist es sehr schwierig, unzugängliche Berührungspunkte in eine Softwareimplementierung eines Verfahrens zu plazieren, außer die Software ist in einem Schutzstück der Hardware geladen. Somit wird es bevorzugt, daß die gesamte Funktionalität, die sich auf das Verfahren bezieht, in ein getrenntes Hardwarestück plaziert wird, das geschützt und ein-

griffssicher ist.

[0049] Wenn das Verfahren ruht, ist es an verschiedenen Stellen unterbrochen. Beispielsweise ist es möglich, ein Verfahren, wie zum Beispiel DES zu nehmen und dasselbe zu unterbrechen. Somit unterbricht das bevorzugte Ausführungsbeispiel der Erfindung DES an mehreren Stellen. Jede dieser Stellen ist ein Berührungspunkt. **Fig.** 2 ist eine schematische Darstellung, die ein allgemeines Berührungspunktprinzip gemäß der Erfindung zeigt.

[0050] In dem DES-Algorithmus ist es sehr nahe am Anfang notwendig, einen Initialisierungsvektor für den Algorithmus zu laden. Typischerweise wird der Initialisierungsvektor mit einem Masterschlüssel oder einem Kombinationsschlüssel oder mit einem gut bekannten oder gemeinschaftlich verwendeten Geheimnis geladen. Dies wird ein Berührungspunkt. Bei diesem Ladeprozeß ist es möglich, entweder die Größe des Wertes zu begrenzen, der geladen wird, oder das Laden festzulegen, so daß, wenn die Taktikeinrichtung vorgibt, daß es als ein Gegenstand der Regierungsrichtlinie notwendig ist, daß alle Initialisierungsvektoren mit einer bestimmten Struktur beginnen, dann diese Struktur in der Tat die Struktur ist, mit der alle Initialisierungsvektoren beginnen. Dies ist ein Beispiel von Berührungspunktdaten.

[0051] Die Daten sind typischerweise einer Längenmaske oder eine Inhaltsmaske, die sagt „Mir ist es egal was Du laden wirst, dies wird wirklich geladen". Oder „Mir ist es egal, welche Größe Du laden möchtest, diese Größe wird geladen". Somit kann ein Berührungspunkt die Daten in der Größe oder im Inhalt beschränken. Solche Beschränkungen werden durch die Taktikeinrichtung vorgegeben. Alles, was die kryptographische Einheit tut, ist, ein Registerpaar, eine Maske (z. B. eine UND-Maske und eine ODER-Maske), zwei Register und einen weiteren Aspekt, der als Berührungspunktgatter bezeichnet wird, zu liefern. Die Berührungspunktdaten werden in diese Register geladen, um diesen Berührungspunkt dieser kryptographischen Einheit zu aktivieren.

[0052] Ein Berührungsgatter, beispielsweise bezüglich des DES, unterbricht den Algorithmus. Somit ermöglicht es die Erfindung, daß ein kritisches Gatter, d. h. ein Gatter, das die Verarbeitung hält, bis die Datenregister geladen sind, als ein Tri-State-Gatter behandelt werden kann, so daß es parametrische Steuerungen gibt, die das Gatter freigeben. Das Gatter ist nicht typischerweise ein binäres Gatter das in einem normalen Zeitgebungssinne arbeitet. Das System erfordert es, daß spezifische Steuerungen für das Gatter aktiviert werden. Wenn keine solche Steuerung vorliegt oder wenn die Steuerung undeutlich oder unbeständig ist, funktioniert das Gatter nicht mehr.

[0053] **Fig.** 3 ist eine schematische Darstellung, die einen spezifischen Berührungspunkt zeigt, der eine Signaturerzeugung gemäß der Erfindung liefert. Durch Unterbrechen des Algorithmus von jeder geraden direkten Funktion, obwohl die Daten in Position sind, verhindert den Betrieb der Funktion weil das Gatter ruht. Somit wird DES vorzugsweise an mehreren Stellen unterbrochen. Auch wenn es möglich wäre, ein Gatter zu zwingen, ist es nach wie vor notwendig, alle anderen solchen Gatter zu finden, um die kryptographische Einheit zu aktivieren. Da sich die Kosten pro TPG verringern ist es möglich, die Anzahl von TPGs zu erhöhen, die bei jedem Verfahren angewendet werden.

[0054] Bezüglich des Berührungspunktgatters als Flußmechanismus ist es unwirksam, ein Gatter zu erzeugen, daß ein Binärzustandsgatter oder ein statisches Gatter ist. Falls das Gatter beispielsweise ein Tri-State-Gatter ist, ist es möglich, das Gatter mit einem Laser zu ätzen und es dauerhaft auf eine Eins oder Null zu setzen. Es ist ferner möglich, die nächsten Gatter zu lokalisieren und dieselben auch auf eine Eins oder eine Null zu setzen. Daher ist es notwendig, ein komplexes Gatter zu erzeugen, daß auf Zufallszahlen anspricht, das hierin als eine Abfrage bezeichnet wird, wobei die kryptographische Einheit eine geeignete Antwort liefert. Somit benötigt das bevorzugte Ausführungsbeispiel der Erfindung eine Abfrage und Antwort zwischen der kryptographischen Einheit und der Taktikeinrichtung. Die kryptographische Einheit erzeugt eine Zufallszahl, beispielsweise eine binäre Zufallszahl, die zu der Abfrage wird, die an die Taktikeinrichtung gesendet wird. Die Abfrage wird verschlüsselt, bevor dieselbe an die Taktikeinrichtung gesendet wird. Die Taktikeinrichtung entschlüsselt die Abfrage, untersucht die Struktur, nimmt das Komplement der Struktur und sendet die Komplementstruktur zu der kryptographischen Einheit, nachdem sie die Mitteilung verschlüsselt. Die kryptographische Einheit entschlüsselt die Mitteilung und bekommt eine Struktur zurück, die zu der Antwort wird.

[0055] Die kryptographische Einheit ist eine Hardwarelösung. Das Funktionieren des Verfahrens in der kryptographischen Einheit wird durch die Berührungspunkte gesteuert. Ein Aspekt der Erfindung ist, daß die kryptographische Einheit in dem Formfaktor einer PCMCIA-Karte geliefert werden kann, in dem Formfaktor eines Chips, der in eine Hauptplatine gelötet ist, oder sogar in dem Formfaktor einer Superzelle, wo die Superzelle direkt zu der CPU wandern kann. Bei allen Ausführungsbeispielen der Erfindung ist die kryptographische Einheit eine vertrauenswürdige und eingriffssichere Komponente des Systems.

[0056] Die Tatsache, daß die kryptographische Einheit vollständig zergliederbar ist, d. h. vollständig freigelegt, ist in der Industrie einmalig. Der Stand der Technik, z. B. der Clip-per-Chip, wird lediglich durch den Gedanken betrieben, daß es schwarze Zellen gibt, die nicht beobachtet oder überprüft werden können. Dies ist bei der kryptographischen Einheit, die hierin beschrieben wird, nicht der Fall, wo es möglich ist, alles in dem Logikfluß zu sehen, d. h. an welchem Punkt Berührungspunktdaten angelegt werden, aber es gibt keinen Weg, durch den Daten entkommen können.

[0057] Es gibt keine Register in der kryptographischen Einheit, die Momentaufnahmen der Daten nehmen oder die Daten halten und mit der Regierung teilen. Dieses Merkmal der Erfindung liefert einen starken Differenziator, da dieselbe in der Lage ist, etwas zu erstellen, das ohne Exportkontrolle versandt werden kann. Die Erfindung ermöglicht es auch, daß kryptographische Einheiten durch eine beliebige Anzahl von Verkäufern hergestellt werden können, ohne Bedenken bezüglich eines Verlustes von Systemintegrität oder -sicherheit. Somit liefert die kryptographische Einheit eine allgemeine Maschine, wo die Taktikeinrichtung als ein „Pförtner" wirkt, der bestimmt, wo und wie Sicherheitsfunktionen geliefert werden.

[0058] Wie es nachfolgend näher erörtert wird, ist die CU an sich nicht personalisiert. Statt dessen ist dieselbe aktiviert. Das heißt, die CU weist eine Seriennummer auf, die Taktikeinrichtungen für diese Seriennummer bestimmt, d. h. die Taktikeinrichtungen sind dazu bestimmt, für eine spezielle kryptographische Einheit zu arbeiten. Sobald die Taktikeinrichtung und die kryptographische Einheit verbunden sind, wandern die Berührungspunktdaten hinüber und die beiden werden eng verbunden. Falls die Taktikeinrichtung von der kryptographischen Einheit entfernt wurde und durch eine andere Flagtaktikeinrichtung ersetzt wurde, würde überhaupt nichts passieren. Das System würde nicht einmal eine Initialisierung durchführen. Die Takteinrichtung kann nirgendwo sonst verwendet werden, und die kryptographische Einheit kann nicht von dieser Taktikeinrichtung getrennt werden.

[0059] Falls der Benutzer der kryptographischen Einheit in ein anderes Land reist und eine Taktikeinrichtung für dieses Land kauft, kann der Benutzer die aktuelle Taktikeinrichtung, z. B. die Vereinigte-Staaten-Taktikeinrichtung, herausnehmen und beispielsweise eine deutsche Taktikeinrichtung einsetzen und die deutsche Taktikeinrichtung und die kryptographische Einheit würden zusammenarbeiten. Somit sind die Taktikeinrichtung und die kryptographische Einheit auf spezielle Weise verbunden, die in jedem Fall unterschiedlich ist, in dem jede Regierung ihre eigene Kryptographietaktik bestimmt.

[0060] Der Stand der Technik sieht nur eine Taktikeinrichtung vor, d. h. eine statische Situation mit einer Taktikeinrichtung, die alle Verwendungen der Kryptographie in der Einheit regelt. Im Gegensatz dazu paßt sich die Erfindung ohne weiteres an jede Taktikeinrichtung oder Richtlinie an. Darüber hinaus liefert die Erfindung mehr als eine Dimension zu einem Zeitpunkt. Beispielsweise ist es möglich, Dreifach-DES für Finanzdienstanwendungen laufen zu lassen, die keine Schlüsseltreuhandanforderungen haben, und gleichzeitig E-Mail mit Schlüsseltreuhand und 40-Bit-DES oder 56-Bit-DE zu verwenden. Die kryptographische Einheit kann beide Kryptographietypen gleichzeitig durchführen, weil eine spezielle Taktikeinrichtung flexibel genug sein kann, um dies zu tun. Dies wird dadurch funktionsfähig, daß, wenn Daten für die Verschlüsselung vorgelegt werden, ein Berechtigungsnachweis geliefert wird, der eine bestimmte kryptographische Dienstklasse bemerkt. Die kryptographische Einheit validiert, daß sie diese Dienstklasse, beispielsweise als Triple-DES, erkennt, und dieselbe erkennt von ihrer Taktikkarte, daß eine solche Dienstklasse für diese Anwendungsdomain autorisiert ist. Die Taktikeinrichtung setzt dann die geeigneten Berührungspunktdaten an den verschiedenen Punkten, die dieser Dienstklasse zugeordnet sind. Das nächste Datenstück kann einen anderen Berechtigungsnachweis aufweisen, d. h. eine andere Dienstklasse.

Grundarchitekturannahmen

– Die CU liefert den Benutzern bei Nichtvorhandensein einer NFC keine kryptographische Funktionen;
– die NFC hat keinen Zugriff auf Benutzerdaten, die in der CU verarbeitet werden;
– die CU oder CUs, die durch eine bestimmte NFC gesteuert werden, ist deterministisch, d. h. jedes Ereignis, jeder Vorgang und jede Entscheidung der CU ist die unvermeidbare Konsequenz von vorhergehenden Ereignissen, die unabhängig von der NFC sind;
– die TPD, die an ein bestimmtes Verfahren angelegt werden, werden durch Berechtigungsnachweise bestimmt, die durch die Anwendung vorgelegt werden, die kryptographische Dienste anfordert;
– die CU, NFC-Aktivierungssequenz kann von Zeit zu Zeit die Teilnahme des ICF-Netzwerksicherheitsserverelements erfordern; und
– ein Primärdrohungsschutz gegen unbefugte Aktivierung der kryptographischen Funktionen ist vorgesehen.

Systemübersicht Einführung

[0061] Eine CU ist ein wesentliches vertrauenswürdiges Element der ICF und liefert grundlegende kryptographische Mechanismen in einem eingriffssicheren Formfaktor. Eine CU, die mit einer ICF-Spezifikation konform ist, entwickelt sich durch drei in sich abgeschlossene Stufen, die als die Herstellungs- und Verteilungsstufe, die Aktivierungsstufe und die Betriebsstufe identifiziert werden. Die ICF-Architektur hat in jeder dieser Stufen eine andere Auswirkung auf die CU: Während der CU-Herstellungs- und Verteilungsstufe wird ein Schwerpunkt auf die Integrität und analytische Freilegung der CU-Logik- und Funktional-Spezifikationen gelegt. In dieser Stufe werden keine Berührungspunktdaten installiert. In der Tat sind solche Daten für einen CU-Hersteller im allgemeinen nicht verfügbar.

[0062] Während der Aktivierungsstufe ist die CU mit einer NFC verbunden, um eine gegenseitig authentifizierte private Sitzung zu erstellen, die dazu dient, TPD zu übertragen und den TPH zu unterstützen.

[0063] Schließlich ist die CU während der Betriebs-

stufe funktional und die Leistungsfähigkeit wird der Hauptfokus.

Herstellungs- und Verteilungsstufe

Schritt 1

[0064] An den Hersteller wird durch eine Zertifizierungsautorität, die durch eine Sicherheitsdomainautorität (SDA = Security Domain Authority) anerkannt ist, eine PvtKey (CU Manufacturer) und ein CU-Herstellerzertifikat ausgegeben. Ein CU-Herstellerzertifikat enthält unter anderem einen öffentlichen Schlüssel, der als PubKey (CU Manufacturer) bezeichnet wird. Öffentliche/Private Schlüssel gehören zu einem sogenannten Schlüsselpaar, das durch ein asymmetrisches Verschlüsselungssystem verwendet wird, wo ein Schlüssel verwendet wird, um zu verschlüsseln oder zu unterschreiben, und der andere Schlüssel verwendet wird, um zu entschlüsseln oder zu verifizieren, daß dies die authentische Signatur ist. Der Verifizierungsschlüssel ist der öffentliche Schlüssel, während der Verschlüsselungsschlüssel der private Schlüssel ist, der geheim gespeichert wird. Die Stärke des asymmetrischen Systems liegt in der Schwierigkeit des Wiederherstellens (re-engineering) des privaten Schlüssels von dem öffentlichen Schlüssel.

[0065] Der legitimierte CU-Hersteller führt die folgenden Aktionen durch:

– Erzeugen einer eindeutigen CU-Seriennummer für jede CU auf der Herstellungslinie.

– Zuweisen eines geheimen Schlüssels, SrtKey (CU-Lot) für jeden Satz erzeugter CUs (z. B. 2000 CUs). Geheime Schlüssel gehören zu dem symmetrischen Verschlüsselungssystem, wo zwei Identitäten ein Vertrauen herstellen, weil dieselben auf ein gemeinschaftliches verwendetes Geheimnis vertrauen.

– Verwenden eines Diversifikationsalgorithmus zum Erzeugen von SrtKey (CU) als eine Funktion der CU-Seriennummer und des SrtKey (CU Lot). Ein solcher Al-gorithmus erzeugt einen eindeutig geheimen Schlüssel für jede CU, unter Verwendung der Seriennummer der CU und eines geheimen Satz-Schlüssels.

– Laden vollständig fähiger, aber ruhender kryptographischer Verfahren (z. B. DES, RSA, MDS, Diffie Hellman) in die CU auf der Herstellungslinie. Die Kryptographie wird unter Verwendung der Berührungspunktlogik ruhend gemacht. Andere kryptographische Verfahren können auch installiert werden, so daß der Bereich der potentialen Stärke für diese Algorithmen erhöht wird.

– Laden der folgenden Informationen in jede CU auf der Herstellungslinie. Die Informationen werden mit Eingriffsschutz installiert, um eine unbefugte Offenbarung dieser Elemente zu vermeiden:

– CU-Herstellerzertifikat-ID
– PvtKey (CU Manufacturer)
– CU-Seriennummer
– SrtKey (CU)

Schritt 2

[0066] Für jeden Satz von hergestellten CUs teilt der CU-Hersteller der/den Sicherheitsdomainautoritäten die folgenden Informationen mit:

– CU-Seriennummer in diesen Satz
– SrtKey (CU-Lot)
– Diversifikationsalgorithmus
– CU-Herstellerzertifikat

Schritt 3

[0067] Ein Kunde bestellt eine CU von einem legitimierten CU-Hersteller oder einem Verteilungskanal für CUs.

[0068] Schritt 4 Auf den Empfang einer Bestellung hin wird eine CU zusammen mit einem NFC-Bestellformular an den Kunden gesendet (vielleicht exportiert).

Schritt 5

[0069] Der Kunde füllt das NFC-Bestellformular aus und sendet es an eine oder mehrere Sicherheitsdomainautoritäten.

[0070] Die Grundelemente auf dem NFC-Bestellformular sind:

– CU-Herstellerzertifikat-ID
– CU-Seriennummer
– kundengewählte einmalige Versand-PIN
– Hostsystem-ID
– Anwendungsdomainautorität-ID
– Anwendungszertifikat-ID
– Anwendungsbeschreibung
– gewünschte Attribute (z. B. Ablaufdatum, Anzahl der Verwendungen, Typen und Stärken der angeforderten Kryptographie)

Schritt 6

[0071] Die Sicherheitsdomainautorität (SDA) empfängt ein NFC-Bestellformular. Unter Verwendung der Informationen von dem NFC-Bestellformular kann die SDA (oder deren befugten Vertreter) eine NFC aktivieren (d. h. personalisieren), um die Anforderung des Kunden zu erfüllen. Die SDA verwendet die CU-Herstellerzertifikat-ID und die CU-Seriennummer zum Identifizieren des Diversifikationsalgorithmus und SrtKey (CU Lot). Unter Verwendung dieser Informationen erzeugt die SDA SrtKey (CU). Es wird davon ausgegangen, daß die Domainautorität Zugriff auf nicht initialisierte (d. h. nicht personalisierte) NFCs hat, die für ihre Spezifikationen erstellt wurden.

[0072] Die SDA initialisiert dann eine NFC durch Installieren der folgenden Informationen:

– CU-Seriennummer, SrtKey (CU), PubKey (CU Manifacturer)
– PIN (1Time Shipping)

SDA-Autorisierungsinformation (1 – n)

– SDA Ids

ADA-Autorisierungsinformation (1 – n)

– ADA-Zertifikat-ID
– PubKey (ADA)

Dienstklassenautorisierungsinformationen (1 – n)

– Dienstklassen-ID
– [Autorisierungsregeln] PvtKey (SDA)
– [NSS-Attribute] PvtKey (SDA)
– [{CU-Berührungspunktdaten} SrtKey (CU)] PvtKey (SDA).

[0073] Dieser Prozeß verriegelt die NFC dauerhaft vor jeder weiteren Modifikation. Die NFC wird, unter Verwendung einer vom Kunden gelieferten einmaligen persönlichen Identifikationsnummer (PIN) für den Transport gesperrt und an den anfordernden Kunden geschickt.
[0074] Bei alternativen Ausführungsbeispielen der Erfindung wird dieser gesamte Schritt online durchgeführt, wobei der Kunde eine NFC installiert, die nur mit einer SDA-ID initialisiert wird, und wo eine kooperierende NSS alle anderen Informationen über das Netzwerk initialisiert. Es ist auch möglich, SDAs, ADAs, CoSs, CoS-Daten oder Berührungspunktdaten online von einem NSS zu aktualisieren. Ferner kann die Erfindung vorsehen, daß eine CU funktional zerstört wird, beispielsweise falls ein Eingriff erfaßt wird, durch Ändern der kritischen Initialisierungsattribute, wie zum Beispiel ID, in der CU, wodurch die CU für immer unbrauchbar gemacht wird.

Schritt 7

[0075] Der Kunde empfängt eine NFC von der SDA. Die vom Kunden gelieferte PIN (1Time Shipping) schützt die NFC während dem Transport, um sicherzustellen, daß nur der ursprüngliche Kunde (d. h. der Kunde, der das NFC-Bestellformular ausfüllt) diese NFC verwenden kann.

Schritt 8

[0076] Der Kunde installiert die NFC in eine NFC-Lesevorrichtung. Im allgemeinen ist die NFC-Lesevorrichtung in die CU eingebaut . Die CU wird dann in das HS installiert, und beendet somit die Herstellungs- und Verteilungsstufe für diese ICF-Elemente.

Aktivierungsstufe

[0077] **Fig.** 4 ist ein Zeitgebungsdiagramm, das das Verhalten einer kryptographischen Einheit während einer Aktivierungsstufe gemäß der Erfindung zeigt. Während der Aktivierungsstufe arbeitet die kryptographische Einheit gemäß dem folgenden Modell:

Grundprinzipien

[0078] Die folgenden Konzepte gelten:
– Die CU arbeitet auf der Basis von Schritten und Modi.
– Ein Modus ist ein interner Zustand der CU. Eine CU kann zu vorhergehenden Modi zurückfallen, auf der Basis von Beispielen, wie zum Beispiel Vertrauensverlust, Versagen der NFC, eine Abfrage anzunehmen, oder Verlust des vitalen Herzschlags. Der aktuelle Modus, in dem eine CU läuft, ist über eine Statusprüfung für die externe Welt zugreifbar.
– Ein Schritt ist die minimale einzelne Sequenz die eine CU steuert, wenn sie in einem bestimmten Modus ist.
– Die CU muß in Modus **3** und in Schritt 4 sein (siehe **Fig.** 4), um die Übertragung der Anfangs-TPD von der NFC anzunehmen.
– Eine deaktivierte CU ist eine Hardwareeinheit, die ein voll funktionsfähiges Siliziumlayout hat (siehe **Fig.** 13), und die das Potential hat, kryptographische Funktionen auszuführen. Die Zusammensetzungsverfahren, die die kryptographischen Funktionen bilden, sind jedoch durch die Berührungspunktgatter deaktiviert.
– Sobald die NFC aus einem Leseschlitz genommen wird, arbeitet die CU in einem Ruhemodus.

Definitionen

[0079] Dieser Abschnitt führt den theoretischen Hintergrund ein, der für die Definitionen erforderlich ist, und auch den Satz von Tools, die verwendet werden, um die Berührungspunktdaten zu installieren.
[0080] Die folgenden Definitionen sind von den ISO/IEC 10181-1 Definitionen abgeleitet und werden hierin für die Interpretation verwendet:
[0081] Sicherheitsautorität: verantwortlich für die Implementierung einer Sicherheitstaktik. Bei dem bevorzugten Ausführungsbeispiel der Erfindung ist die erste Sicherheitsautorität von Belang die NSA, d. h. die US National Security Agency.
[0082] Sicherheitstaktik: ein Satz von Regeln, die die Verwendung kryptographischer Funktionen innerhalb einer Anwendungsdomain beschränkt. In Verbindung mit der Erfindung hierin sind dies die Regeln, durch die die Sicherheitsfunktion zur Zufriedenheit der Sicherheitsautorität erhalten wird, wie es durch den Berührungspunktlebenszyklus dargestellt ist. Bei dem bevorzugten Ausführungsbeispiel der Erfindung werden nur die Regeln, die auf spezielle Sicherheitsbereiche angewendet werden, berücksichtigt. Diese identifizierten Sicherheitsdomains sind Frankreich, Großbritannien, Deutschland und Japan. Die jeweiligen Autoritäten sind SCSSI, CSG, BSI und MITI.
[0083] Sicherheitsdomain: ein Satz von Elementen unter einer bestimmten Sicherheitstaktik, die durch

eine einzige Sicherheitsautorität für einige spezifische sicherheitsrelevante Aktivitäten verwaltet wird. Wo die Hauptsicherheitsdomain, die berücksichtigt wird, beispielsweise die Vereinigten Staaten sind, sind die Elemente, die gesteuert werden sollen, die CUs.

[0084] Regeln: diese werden von der Sicherheitstaktik abgeleitet. Sie übersetzen eine Beschränkung auf Aktivitäten und Elemente. Als ein Beispiel für eine solche Regel: Beschränke den DES-Verschlüsselungsmechanimus für Anwendungen, die durch ein ADA-Anwendungsdomainautorität des Typs A ausgewählt wird, auf internationale Übertragungen mit einer Schlüssellänge von 128 Bit.

[0085] Eine Regel-ri- ist das Ergebnis der folgenden Formel:

r1 = T(Taktik1)r3 = (r1 UND r2) ODER T(Taktik3)

r2 = T(Taktik2)r4 = ...

[0086] Berührungspunktdaten (tpd): das Ergebnis der Übersetzung der natürlichen Sprache, die semantisch ausgedrückt wird, von expliziten und genauen Regeln (ri) in einen eindeutigen Ziffern- oder Chiffre-Strom. Genauer gesagt machen die TPD eine Regel spezifisch für eine kryptographische Funktion. Darüber hinaus liefern dieselben eine parametrische Steuerung über einen Berührungspunkt zu einen bestimmten Zeitpunkt, die als TPDI bezeichnet wird. Die TPDI ist die Übersetzung zu einem Zeitpunkt t0 einer Regel ri für einen spezifischen Berührungspunkt. Sobald die TPDI in eine NFC geladen ist, kann eine TPDI jede Anwendung freigeben, die eine äquivalente Erlaubnis hat, die als die kryptographische Dienstklasse (COS) bezeichnet wird, von ihrer Anwendungsdomainautorität (ADA). Die TPDI-Übersetzung kann durch die folgende Gleichung dargestellt werden: Für einen Algorithmus, der in vier Berührungspunkte tp1, tp2, tp3 und tp4 unterteilt ist:

tdp1 = F1 (t0, r1, tp1), wobei F1 für eine kryptographische Funktion steht

tpd2 = F1 (t0, r1, tp2),

tpd3 = F1 (t0, r1, tp3),

tpd4 = F1 (t0, r1, tp4),

tpd5 = F2 (t0, r2, tp5),

usw.

[0087] Durch Erweiterung sind NFCs durch die SDA, mit allen potentiellen Kryptographiedienstklassen vorgefertigt, zum Freigeben der ADA zum Steuern der Verwendung der Kryptographie innerhalb ihres Bereichs. Die TPDIs sind nach Dienstklasse zusammengefaßt, bevor dieselben verschlüsselt werden und mit dem privaten Schlüssel der SDA unterschrieben werden, wie es in dem obigen SCHRITT 6 spezifiziert ist.

[0088] COS: eine Kryptographiedienstklasse ist ein externer Identifizierer, der zwischen einer SDR und den dazugehörigen ADAs gemeinschaftlich verwendet wird, der verwendet wird, um auf die Implementierung einer Regel zu verweisen. Eine bestimmte Regel i wird eine Dienstklasse i, sobald dieselbe einer ADA angeboten wird, um als kryptographische Funktion für eine Klasse von Anwendungen zugewiesen zu werden.

[0089] Diese Situation kann mit der folgenden Gleichung übersetzt werden:

COS1 entspricht tpd1 ...tpd4, gilt für COS1,

COS2 entspricht tpd5 ...tpd7, gilt für COS2,

usw.

[0090] Daher gibt das Entkoppeln der Dienstklasse von der potentiellen Schwankung der Taktikeinrichtungen dem gesamten Modell eine starke Flexibilität.

[0091] Eine ADA empfängt eine zertifizierte Liste von Dienstklassen (COS1, COS2, COS5, COS7, COS8) von der SDA als eine authentifizierte Abordnung zum Zuweisen der Kryptographie.

[0092] **Fig.** 5 ist eine schematische Darstellung, die eine Dienstklasseninstallation gemäß der Erfindung zeigt. Die Fig. stellt die Beziehung zwischen der COS, der TPD, der ADA und der SDA (wie es oben erörtert wurde).

Die Beziehungen zwischen der ADA und der SDA

[0093] **Fig.** 6 ist eine schematische Darstellung, die eine Sicherheitsdomainautorität, Anwendungsdomainautorität und eine Anwendungsverschachtelung gemäß der Erfindung zeigt. Die SDA gibt ein Token (verschiedene Standards können als Fälle des Tokens angewendet werden), mit den zertifizierten Dienstklassen an die ADAs aus, die innerhalb ihrer Rechtssprechung liegen, wie es durch den Kreis gezeigt ist, der jede SDA umgibt. Eine solche Rechtssprechung könnte sich schließlich über mehrere Länder oder Gruppen erstrecken (z. B. NAFTA, EG oder G7). Beispielsweise könnten Token dieser Art die Vorgabewerte für die internationale Kommunikation erzeugen. Der grundlegende Wert dieser Abordnung ist, daß eine Anwendung in einer Anwendungsdomain erzeugt und verteilt werden kann, ohne vorhergehende Anfrage an die SDA für eine bestimmte Kryptographieebene.

Betriebsstufe

[0094] Der TPD-Lebenszyklus, der mit der NFC gekoppelt ist

[0095] **Fig.** 7 ist eine schematische Darstellung, die einen Berührungspunktdatenlebenszyklus zeigt, einschließlich Erzeugung, Installation/Verteilung und Laden gemäß der Erfindung.

[0096] Wie es in **Fig.** 7 gezeigt ist, ist ein TPD-Lebenszyklus in vier Hauptphasen unterteilt:

Erzeugung

[0097] Die TPD werden durch die Bereichsautorität bei zwei unterschiedlichen Sicherheitsstufen in dem Lebenszyklus erzeugt:

– erstens an der Herstellungs- und Verteilungsstufe der NFC; und

– zweitens an der Betriebsstufe durch den NSS (wie

es in **Fig.** 8 gezeigt ist).

Installation

[0098] Das Ergebnis der Erzeugungsfunktion wird sofort bei der Personalisierungszeit während der Herstellungs- und Verteilungsstufe in der NFC installiert.

[0099] Aktualisierung/Austausch

[0100] **Fig.** 9 ist eine schematische Darstellung, die einen Berührungspunktdatenlebenszyklus zeigt, einschließlich einer Aktualisierung gemäß der Erfindung.

[0101] Wie es in **Fig.** 9 gezeigt ist, überträgt der NSS, der für die Erzeugung einer neuen Version der Taktikregeln verantwortlich ist, das Ergebnis nur während der Betriebsstufe über das Netzwerk zurück zu der CU.

Einzelheiten der kryptographischen Einheit-Funktionselemente

[0102] **Fig.** 10 ist eine schematische Darstellung, die die Funktionselemente einer kryptographischen Einheit gemäß der Erfindung zeigt. Diese Elemente der Erfindung werden nachfolgend näher erläutert.

Laden

[0103] **Fig.** 11 ist eine schematische Darstellung, die eine Ladesequenz gemäß der Erfindung zeigt. Zu dem Zeitpunkt, zu dem die NFC die Abfrage mit der CU beendet, wird die COS per Anwendung in die Ladevorrichtung installiert, und entschlüsselt, bevor dieselbe in die Gatter gedrückt wird. Sobald die Logik aktiviert ist, gibt der Herzschlag die Verbindungen zwischen den zusammensetzenden Elementen frei, und die Verschlüsselungsverfahren sind bereit, um ausgeführt zu werden.

[0104] Es sollte für einen Fachmann auf diesem Gebiet klar sein, daß Verfahren auf viele verschiedene Arten in die CU geladen werden können. Weil das Verfahren von jedem Element in der ICF geladen werden kann, auf der Basis der Autorisierung jeder Kombination von vertrauenswürdigen Elementen, kann solches Laden als dynamisch angesehen werden. Beispielsweise kann das Hostsystem ein Verfahren in die CU laden, der NSS kann ein Verfahren in die CU laden, oder die Taktikeinrichtung kann ein Verfahren in die CU laden, alle unter Überwachung der Taktikeinrichtung. Ferner können die Verfahren in einem ruhenden Zustand in der CU sein, wo jedes von mehreren Verfahren durch vertrauenswürdige Elemente der ICF aktiviert wird, z. B. die Taktikeinrichtung oder den NSS.

Funktionseinzelheiten

[0105] Die CU schaltet in ihren sicheren Modus **4** – Schritt 4 (siehe **Fig.** 4). Die folgenden Interaktionen finden zwischen den drei Funktionselementen statt (siehe **Fig.** 11). Für diese Figur und auch für **Fig.** 12 und 13 wird jeder Schritt in einer Sequenz der Operation in der Figur durch eine eingekreiste Zahl angezeigt, die die Position in der Figur der Aktion zeigt, die erklärt wird.

Schritt 1

[0106] Die Hüllen, die während der Inbetriebnahme des Sitzungsschlüssels verwendet werden, werden in dem Comm-I/O-Element gehandhabt. Dann werden die relevanten COS von der Hülle extrahiert und die verschlüsselten tpds werden zunächst in Kryptographische-Steuerungs- und Dienstklassen-Attribute aufgeteilt, bevor dieselben in das Ladevorrichtungselement gedrückt werden.

Schritt 2

[0107] Die Ladevorrichtung aktiviert die dynamische Logikzustandsfreigabelogik pro Gatter – eines nach dem anderen – mit spezifischen Ausführungs- und Zeitgebungsbeschränkungen und programmatischen Verbindungssequenzen, um die kryptographischen Mechanismen vorübergehend zu sperren.

Schritt 3

[0108] Sobald alle tpd installiert sind, sperrt die Ladevorrichtung die beschränkten Zugriffe der dynamischen Zustandsfreigabelogik. Die CU-Ladevorrichtung erzeugt dann Installationssteuersequenzen, die in dem Systembetriebskern durch die sichere Ladevorrichtung interpretiert werden. Zwei Sequenzen werden für den CU-Treiber (Neuinstalliertreiber, Signatur berechnen) gesendet, und zwei Sequenzen werden für die DB-Laufzeit (Neuinstallierlaufzeit, Signatur berechnen) gesendet.

[0109] Der erzeugte Hashwert des neu installierten Treibers wird zu der CU-Ladevorrichtung zurück gesendet, die dann gegen die DB-Laufzeit Signatur verifiziert. Wenn beide Signaturen korrekt sind, können die Anwendungen kryptographische Dienste aufrufen.

TPD-Laden-Fluß von Ereignissen

[0110] Der folgende Abschnitt konzentriert sich auf die Schritte, die erforderlich sind, und die Aktionen, die durch die drei Funktionselemente durchgeführt werden, um die TPDI in einen Satz von Regeln zu übersetzen, die an die kryptographischen Module der CU angewendet werden können. **Fig.** 12 ist eine schematische Darstellung, die einen Fluß von Ereignissen für einen Berührungspunktdatenladesequenz gemäß der Erfindung zeigt.

Schritt 1

[0111] Nachdem die Sitzungsschlüssel eingerichtet wurden, und der Herzschlag zwischen den beiden Elementen synchronisiert ist, trägt die NFC alle tpdi, die sich auf alle COS beziehen, eines nach dem anderen in das Kommunikationselement.

Schritt 2

[0112] Die Attribute der COS und die tpdi werden von den Inhalten der Hülle extrahiert. Solche Attribute können beispielsweise den Algorithmustyp, die Anzahl der Verwendungen oder das Ablaufdatum umfassen, aber auch solche Operationen, wie zum Beispiel Übersetzen der Regel, Verwenden eines symmetrischen Schlüsselalgorithmus mit einer 168-Bit-Treuhand oder -Nicht-Treuhandschlüssellänge. Die Beschränkungsströme in den tpdi bei dem bevorzugten Ausführungsbeispiel der Erfin-dung sind wie die Schlüssel treuhandmäßig organisiert werden, oder unter welchen Schema, als ein Beispiel.

Schritt 3

[0113] Es ist die Rolle der Ladevorrichtung, die COS-Identität in die COS-Aktivzone zu drücken, und das Ergebnis der Datenvaliditätsprüfung und der Beschränkungsinformationen in das Beschränkungsgatter.

Schritt 4

[0114] Der Beschränkungsziffernbitstrom wird nun im Klartext in eine Beschränkungsleitung gedrückt.

Schritt 5

[0115] Der Klartext-Bitstrom, der das Ergebnis der Beschränkungsleitung, die eine n-Schritt-Permutation verwendet, wird verwendet, um das kryptographische Modul zu programmieren.

Schritt 6

[0116] Als ein Beispiel ist das kryptographische Modul als Dreifach-DOS programmiert und ist bereit, eine 168-Schlüssellänge anzunehmen, um die Verschlüsselung laufen zu lassen. Sobald Schritt 6 erreicht ist, wartet die Ladevorrichtung auf eine Bestätigung von einem ersten Modul bevor dieselbe zu einem zweiten Modul fortschreitet.

Schritt 7

[0117] Falls aus irgendeinem Grund das zweite Modul nicht für COSs aktiviert ist, ist die Leitung leer und erzwingt einen Nicht-Programmier-Zustand.

Schritte 8–12

[0118] Fortsetzung wie für die Beschränkung 1 (Schritte 4–6) für alle anderen COSs.

Anwendungsverwendung – Fluß von Ereignissen

[0119] **Fig.** 13 ist eine schematische Darstellung, die einen Fluß von Ereignissen für eine Anwendung a1 zeigt, die das Recht hat, eine kryptographische Funktion 1 gemäß der Erfindung zu verwenden: die unterschriebene Anforderung derselben umfaßt eine COS-ID, die mit derjenigen übereinstimmt, die in der CU installiert ist. Die Anwendung a1 hat das Recht, die kryptographischen Funktionen auszuführen. Eine weitere Anwendung, die eine weitere COS anfordert, muß in die Warteschlange gesetzt werden, um einen Zugriff auf diese Kryptofunktionen zu erhalten.

Schritt 1

[0120] Die Anwendung a1 präsentiert die Schlüssel, die verwendet werden sollen, oder wählt einen Index aus zum Wiedergewinnen der Schlüssel, die für den kryptographischen Ablauf verwendet werden sollen.

Schritt 2

[0121] Die Präsentation der Schlüssel löst aus, daß die a1-Identität dem Beschränkungsgatter präsentiert wird. Falls die Zeit und das Datum der Verwendung oder die Anzahl von Verwendungen nach wie vor mit den eingestellten Steuerinformationen übereinstimmt, aktiviert das Ausgangssignal das Auftreten des der nächsten Schritts. Falls alle diese Bedingungen nicht erfüllt sind, sind die Daten, die präsentiert werden, für das kryptographische Modul nicht sichtbar.

Schritt 3

[0122] Dieses Signal öffnet/schließt den Eingangsdatenstrom.

Schritt 4

[0123] Die Datenmasse läuft durch das kryptographische Modul, die dieselben nun mit dem Schlüssel verschlüsselt, der in dem obigen Schritt 1 ausgewählt wurde.

Schritt 5

[0124] Das Ergebnis wird der Anwendung a1 in einer Datenzone präsentiert.

Verfallsfunktion

[0125] Jede dieser Mitteilungen, die zwischen der kryptographischen Einheit und der Taktikeinrichtung

gesendet wird, wird unter Verwendung eines Schlüssels verschlüsselt, der sich fortlaufen ändert. Dies ermöglicht es dem System, eine Progression zu erzeugen, die nicht gestört werden kann, weil sich der Schlüssel immer ändert. Der Wert ki (wobei ki eine der Mitteilungen ist) ist gleich einer Funktion der Sitzungssequenznummer (RN). Diese Mitteilungen begannen mit einem Zufallspunkt (z. B. 1010, der eine Zufallszahl ist, die die erste Sequenzzahl war, die zwischen der Taktikeinrichtung und der kryptographischen Einheit gesendet wurde. Die Taktikeinrichtung sendet eine Antwort an die kryptographische Einheit, die die Zahl, d. h. 1011, inkrementiert. Das System setzt das Sequenzieren von diesem Zufallspunkt fort. Die Funktion des Werts ki ist eine Funktion dieser Zufallszahl und k, wobei k während der Initialisierungsphase (wie oben erörtert) bestimmt wird, und ein eindeutiger Schlüssel ist, den die Taktikeinrichtung und die kryptographische Einheit jetzt gemeinschaftlich verwenden.

[0126] Um den Schlüssel an jedem Punkt ki zu kennen oder diesen Schlüssel vorherzusagen, ist es notwendig, die Seriennummer der Mitteilung, RN, und k, die ursprüngliche Nummer, zu kennen. Außerdem hat die Funktion einen Verfallswert. Man nehme beispielsweise an, daß die Taktikeinrichtung und die kryptographische Einheit seit einiger Zeit in Kommunikation sind und bei der Zahl 2084, d. h. dem Wert von RN angekommen sind. Wo ein Eindringling einen großen Teil der Mitteilungen erfaßt hat und zurückkommen möchte und die erste Mitteilung bekommen möchte, funktioniert die Funktion nicht, falls der ersetzte Wert mehr als ein Delta von 10 von der tatsächlichen Nummer entfernt ist. Somit ist ki nur gültig, wenn RN geringer oder gleich 10 von dem nächsten oder vorhergehenden RN ist.

[0127] Mit der Verfallsfunktion können die Taktikeinrichtung und die kryptographische Einheit eine Mitteilung jedes Typs weiterleiten, die unter Verwendung von ki verschlüsselt ist. Mit einem Brute-Force-Angriff auf eine Mitteilung kann es möglich sein, fortzufahren und fünf Tage lang zu arbeiten, und eine Mitteilung zu durchbrechen, um ki zu bekommen. Dies ist dann jedoch der Zustand des Schlüssels von vor zwei Tagen. Die Kenntnis dieses Schlüssels und selbst die Kenntnis dieser Funktion können nicht umgekehrt werden, um den Wert von k zu identifizieren. Selbst wenn k und ki bekannt sind ist der berechnete Wert mehr als 10 von dem aktuellen Wert entfernt.

[0128] Ein Wert, wie zum Beispiel 10, wird bei einem bevorzugten Ausführungsbeispiel der Erfindung gewählt, weil ein legitimiertes System durch einen Jitter aus einer Synchronisation fallen könnte, beispielsweise aufgrund eines Leistungsausfalls oder falls jemand die Taktikeinrichtung herausnimmt, kurz bevor dieselbe die Nummer in ihrem statischen RAM aktualisieren konnte. Plötzlich wird das System wieder eingeschaltet, aber das System geht nie erneut zurück zu Null. Wenn das System wieder eingeschaltet wird, wird davon ausgegangen, daß das System mit ki beginnt. Der Wert könnte jedoch versetzt sein, daher ist die Zahl in dem Algorithmus modifizierbar, zum Beispiel um 10.

[0129] Ein wichtiger Aspekt der Erfindung ist, daß das System der Taktikeinrichtung vertraut, aber der kryptographischen Einheit nicht wirklich vertraut. Ab und zu kann die Taktikeinrichtung die Sequenznummer ändern. Somit kann die Taktikeinrichtung normalerweise die Sequenznummer immer um Eins inkrementieren, und dann gibt dieselbe ab und zu eine andere Zufallszahl aus. Wenn dieselbe dies tut, empfängt die kryptographische Einheit die Anzahl in der Mitteilung, weil die Mitteilung unter Verwendung von ki verschlüsselt wurde, was das System synchronisiert. Wenn die andere Seite plötzlich sieht, daß die Sequenznummer springt, ist die Mitteilung, die empfangen wird, gültig, weil dieselbe in dem Strom war, mit dem richtigen nächsten Schlüssel verschlüsselt wurde und nur die Sequenznummer einen Sprung durchführt. Die kryptographische Einheit folgt diesen Sprung, weil sie gerade eine Mitteilung zurück an die Taktikeinrichtung senden wollte. Daher springt das System regelmäßig absichtlich über den Verfallswert, z. B. 10, für den Fall, daß der Wert vor den zehnten Mitteilung verschlüsselt wurde. Dieser Sprung kommt nur von der Taktikeinrichtung. Eine kryptographische Einheit weiß, daß es von Zeit zu Zeit einen Sprung gibt, aber wenn die Taktikeinrichtung je einen Sprung erlebt, wird sie funktionieren. Das Intervall für den Sprung kann völlig zufällig sein und der Betrag des Sprungs kann nach oben oder nach unten oder in jede Richtung sein.

Kryptographische Module Prinzipien

Beispiel 1: Berührungspunktdaten deaktivieren die Verwendung eines Algorithmus.

[0130] Die durch die Taktikkarte aktivierte Firmware ist in einer Schichtweise strukturiert, und in der Schicht **1** installiert, die den Zugriff zu dem Algorithmus verhindert. Ein spezifischer Code, der mit dieser Funktion verwandt ist, testet das Zertifikat der Anwendung, um zu Bestimmen, ob dieselbe mit der COS übereinstimmt, die derzeit installiert ist. Falls die COS und die Zertifikatinhalte übereinstimmen, tritt eine Ausführung auf; falls es keine Übereinstimmung gibt, wird die Anforderung abgelehnt.

Beispiel 2: Berührungspunktdaten erzwingen die Verwendung einer 128-Bit-Schlüssellänge für einen spezifischen Algorithmus.

– Installieren eines Filtermechanismus in der Schicht **1**, der einen Steuerfluß aktiviert.
– Bereitstellen von Zugriff zu einem Schlüsselladem echanismus, der eine aktive Prüfung auf der Schlüssellänge durchführt. Folgendes sollte auftreten:
– Falls die Schlüssellänge y größer als x, x ist, das

durch die Taktikkarte spezifiziert wurde, Zurücksenden eines Fehlers, der anzeigt, daß es die bestehende Taktikeinrichtung dem System nicht erlaubt, mit der Länge y zu arbeiten.
– Zu diesem Zeitpunkt würde es nur ein System auf der Basis eines geheimen Schlüssels der CU erlauben, fortzufahren. Dies ist fraglich, weil die Partner- bzw. Peer-Entitäten bisher noch nicht auf diese spezifischen Schlüssel synchronisiert sind.
– Der asymmetrische Algorithmus ist viel leichter, weil kein äquivalentes Schlüsselpaar erzeugt werden kann, ohne eine Benachrichtigung oder Installation eines Elementes des Paars.
– Keine Aktion kann durchgeführt werden.

Taktikeinrichtung in Kraft halten

[0131] Ein wichtiger Teil der ICF ist die NFC-CU-Beziehung. Es ist notwendig, den Herzschlag funktionsfähig zu halten, wobei die Abfragen zwischen der CU und der NFC synchronisiert sind. Der NSS kann diese Taktiken nach einer umhüllten Abfrage ändern.

Geltendmachen der Verwendung eines Schlüsseltreuhandschemas

[0132] Die Schicht **1** ist bei einer Implementierung der Ort, wo eine spezifische Firmware installiert ist, um das Schema erneut zu dem Zeitpunkt auszuführen, wenn der Schlüssel geladen wird. Der Schlüssel **3** spielt die Rolle des Schlüsselunterbrechers.
[0133] Die Schicht **1** ist der Ort, wo spezifische Vorgabefunktionen ausgeführt werden: vorgegebene symmetrische/asymmetrische Algorithmen plus Verschlüsselungsschlüssellänge, Vorgabesignaturerzeugung und Verifikationsalgorithmen, ein Vorgabetreuhandschema.

COS Attributverwaltung

[0134] Der COS-Attributteil der Berührungspunktdaten besteht aus den folgenden Informationen:
– Algorithmustyp (DES, Dreifach-DES, RSA, ...),
– Schlüssellänge,
– maximale Anzahl der Verwendungen, und
– Ablaufdatum.

[0135] Diese Liste ist nicht erschöpfend und es ist ziemlich wichtig, daß auf dieser Ebene eine gewisse Flexibilität beibehalten wird. Aus diesem Grund sollte das Verarbeiten und Prüfen der Attribute auf der Ebene der geschützten Schicht **1** durchgeführt werden.
[0136] Obwohl die Erfindung hierin mit Bezugnahme auf das bevorzugte Ausführungsbeispiel beschrieben ist, wird ein Fachmann auf diesem Gebiet ohne weiteres erkennen, daß andere Anwendungen für die hierin aufgeführten eingesetzt werden können, ohne von dem Schutzbereich der vorliegenden Erfindung abzuweichen. Folglich soll die Erfindung nur durch die angehängten Ansprüche beschränkt werden.

Patentansprüche

1. Eine kryptographische Einheit (**14**), die folgende Merkmale umfaßt:
zumindest eine kryptographische Einrichtung, die auf eine oder mehrere vorbestimmte Arten an einer Mehrzahl von Berührungspunkten deaktiviert wird; und
eine dynamische Zustandsfreigabelogik an jedem Berührungspunkt, die ein Berührungspunktgatter bildet, das eine regelmäßige Neukonfiguration erfordert, um solche Berührungspunkte in einem freigegebenen Zustand zu halten,
wobei die regelmäßige Neukonfiguration durch ein fortlaufendes Protokoll erreicht wird, das zwischen der kryptographischen Einheit (**14**) und einer Taktikeinrichtung (**12**) errichtet wird,
wobei die Taktikeinrichtung (**12**) mehrere Parameter aufweist, die durch eine autorisierte Entität eingestellt sind, wobei diese Parameter die Identität der kryptographischen Einheit und die Protokollparameter umfassen, und
wobei das fortlaufende Protokoll gemäß denjenigen Parametern durchgeführt werden muß, die der kryptographischen Einheit (**14**) durch die Taktikeinrichtung (**12**) präsentiert werden, wenn dieselben verbunden sind.

2. Die kryptographische Einheit gemäß Anspruch 1, die ferner folgendes Merkmal umfaßt: Berührungspunktdaten, die den Berührungspunkten zugeordnet sind, um eine parametrische Steuerung über die Funktionsweise jedes Berührungspunkts zu liefern.

3. Die kryptographische Einheit gemäß Anspruch 1 oder 2, bei der jede kryptographische Einrichtung durch mehrere Berührungspunkte innerhalb dieser Einrichtung gesteuert wird.

4. Die kryptographische Einheit gemäß einem der Ansprüche 1 bis 3, bei der alle Berührungspunktgatter für eine bestimmte kryptographische Einrichtung in einem freigegebenen Zustand sein müssen, um diese Einrichtung zu aktivieren.

5. Die kryptographische Einheit gemäß einem der Ansprüche 1 bis 4, bei der das fortlaufende Protokoll zwischen der kryptographischen Einheit und der Taktikeinrichtung (**12**) errichtet wird, um eine dynamische konstante Auffrischung und eine Zustandsbestimmung für die kryptographische Einheit (**14**) zu liefern.

6. Die kryptographische Einheit gemäß einem der Ansprüche 1 bis 5, wobei die kryptographische Einheit für den Betrieb in einer internationalen Kryptographiegrundstruktur angepaßt ist, die vier Dienst-

elemente aufweist, die jeweils unterschiedliche Diensttypen anbieten, wobei die Dienstelemente die Taktikeinrichtung (**12**), die kryptographische Einheit (**14**), ein Hostsystem (**16**) und einen Netzwerksicherheitsserver (**18**) umfassen.

7. Die kryptographische Einheit gemäß Anspruch 6, bei der die kryptographische Einheit bei der Abwesenheit der Taktikeinrichtung keine kryptographischen Funktionen liefert.

8. Die kryptographische Einheit gemäß Anspruch 6 oder 7, bei der die Taktikeinrichtung geeignete Berührungspunktdaten an verschiedenen Punkten einstellt, die einer Dienstklasse zugeordnet sind, um jede einer Mehrzahl von kryptographischen Dienstklassen freizugeben.

9. Die kryptographische Einheit gemäß einem der Ansprüche 1 bis 8, die ferner folgendes Merkmal umfaßt:
einen Abfrage-/Antwortmechanismus zum Sichern einer Kommunikation zwischen der kryptographischen Einheit und einer Freigabetaktikeinrichtung.

10. Die kryptographische Einheit gemäß einem der Ansprüche 1 bis 9, die ferner folgendes Merkmal umfaßt:
eine Abklingfunktion zum dynamischen Ändern eines Abfrage-/Antwortschlüssels.

11. Die kryptographische Einheit gemäß Anspruch 10, bei der die Abklingfunktion ferner folgendes Merkmal umfaßt:
eine Einrichtung bei der Taktikeinrichtung (**12**) zum zufälligen Ändern des Abfrage-/Antwortschlüssels.

12. Die kryptographische Einheit gemäß Anspruch 10 oder 11, bei der die Abklingfunktion ferner folgendes Merkmal umfaßt:
einen festen Wertversatz, der einen Bereich von annehmbaren Werten für den Abfrage-/Antwortschlüssel definiert.

13. Die kryptographische Einheit gemäß einem der Ansprüche 9 bis 12, bei der der Abfrage-/Antwortmechanismus nicht wiederholend und/oder nicht vorhersagbar ist.

14. Die kryptographische Einheit gemäß einem der Ansprüche 9 bis 13, die ferner folgendes Merkmal umfaßt: einen Zertifikatsmechanismus zum Authentifizieren der kryptographischen Einheit.

15. Die kryptographische Einheit gemäß Anspruch 14, bei der der Zertifikatsmechanismus nicht wiederholend und/oder nicht vorhersagbar ist.

16. Die kryptographische Einheit gemäß Anspruch 14 oder 15, bei der der Zertifikatsmechanismus eine Privileghierarchie implementiert.

17. Die kryptographische Einheit gemäß einem der Ansprüche 1 bis 16, bei der die kryptographische Einrichtung dynamisch in die kryptographische Einheit geladen ist.

18. Die kryptographische Einheit gemäß einem der Ansprüche 6 bis 17, bei der sich zumindest eine der kryptographischen Einrichtungen in der kryptographischen Einheit befindet, und ruhend ist, bis sie durch die Taktikeinrichtung aktiviert wird.

19. Die kryptographische Einheit gemäß einem der Ansprüche 1 bis 18, wobei die kryptographische Einheit ein Initialisierungsattribut umfaßt.

20. Die kryptographische Einheit gemäß Anspruch 19, wobei die kryptographische Einheit durch die Änderung des Initialisierungsattributs funktional zerstört wird.

21. Ein Verfahren zum Verhindern einer nichtautorisierten Verwendung von kryptographischen Funktionen, das folgende Schritte umfaßt:
Liefern einer kryptographischen Einheit, die zumindest ein kryptographisches Verfahren aufweist, das auf eine oder mehrere vorbestimmte Arten an einer Mehrzahl von Berührungspunkten deaktiviert ist, wobei jedes kryptographische Verfahren durch mehrere Berührungspunkte innerhalb des Verfahrens gesteuert wird; und
Liefern einer dynamischen Zustandsfreigabelogik an jedem Berührungspunkt, die ein Berührungspunktgatter bildet, das eine regelmäßige Neukonfiguration erfordert, um die Berührungspunkte in einem freigegebenen Zustand zu halten,
wobei die regelmäßige Neukonfiguration durch ein fortlaufendes Protokoll erreicht wird, das zwischen der kryptographischen Einheit (**14**) und einer Taktikeinrichtung (**12**) errichtet wird,
wobei die Taktikeinrichtung (**12**) mehrere Parameter aufweist, die durch eine autorisierte Entität eingestellt sind, wobei diese Parameter die Identität der kryptographischen Einheit und die Protokollparameter umfassen, und
wobei das fortlaufende Protokoll gemäß denjenigen Parametern durchgeführt werden muß, die der kryptographischen Einheit (**14**) durch die Taktikeinrichtung (**12**) präsentiert werden, wenn dieselben verbunden sind.

Es folgen 13 Blatt Zeichnungen

Anhängende Zeichnungen

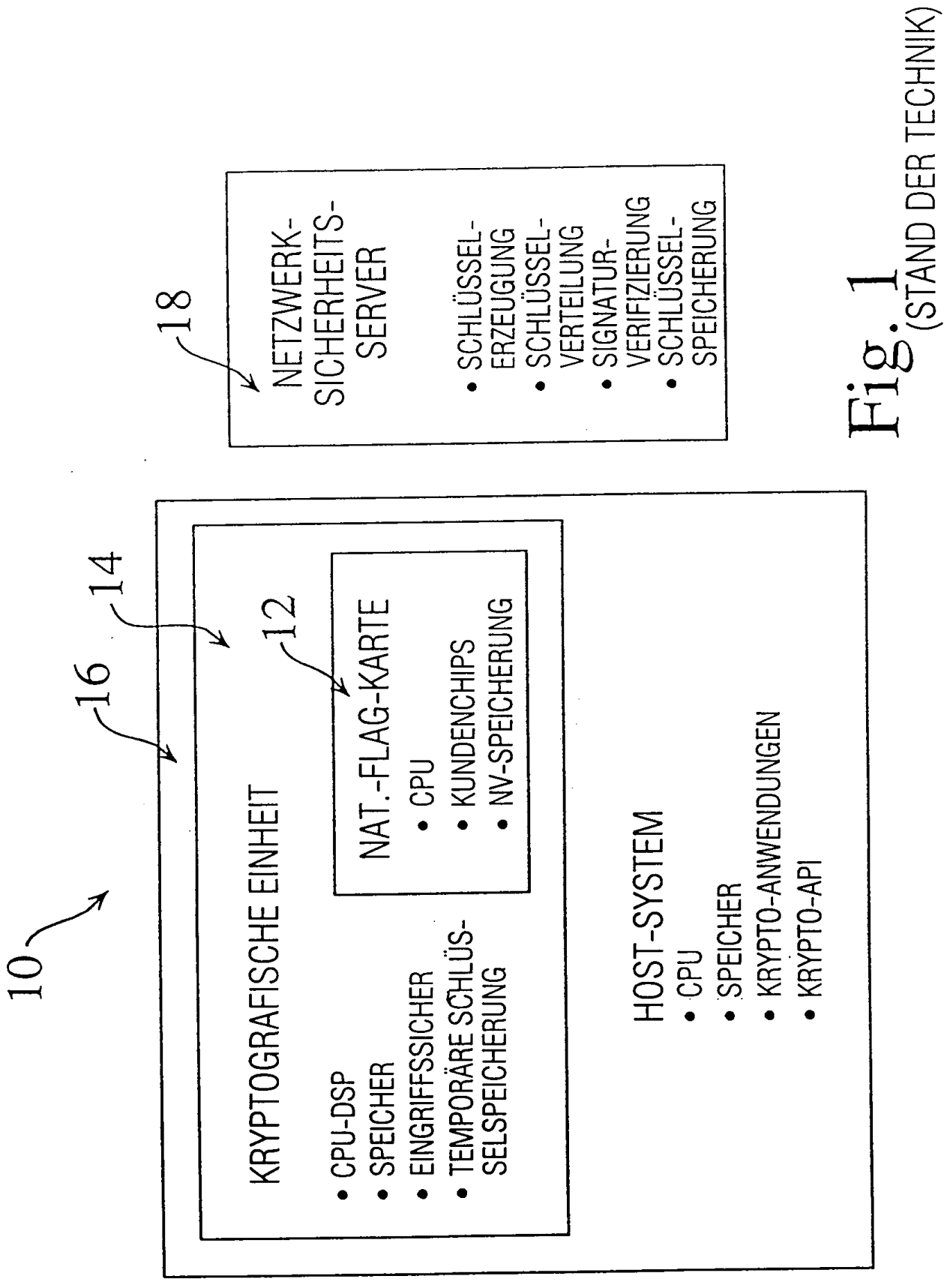


Fig. 1 (STAND DER TECHNIK)

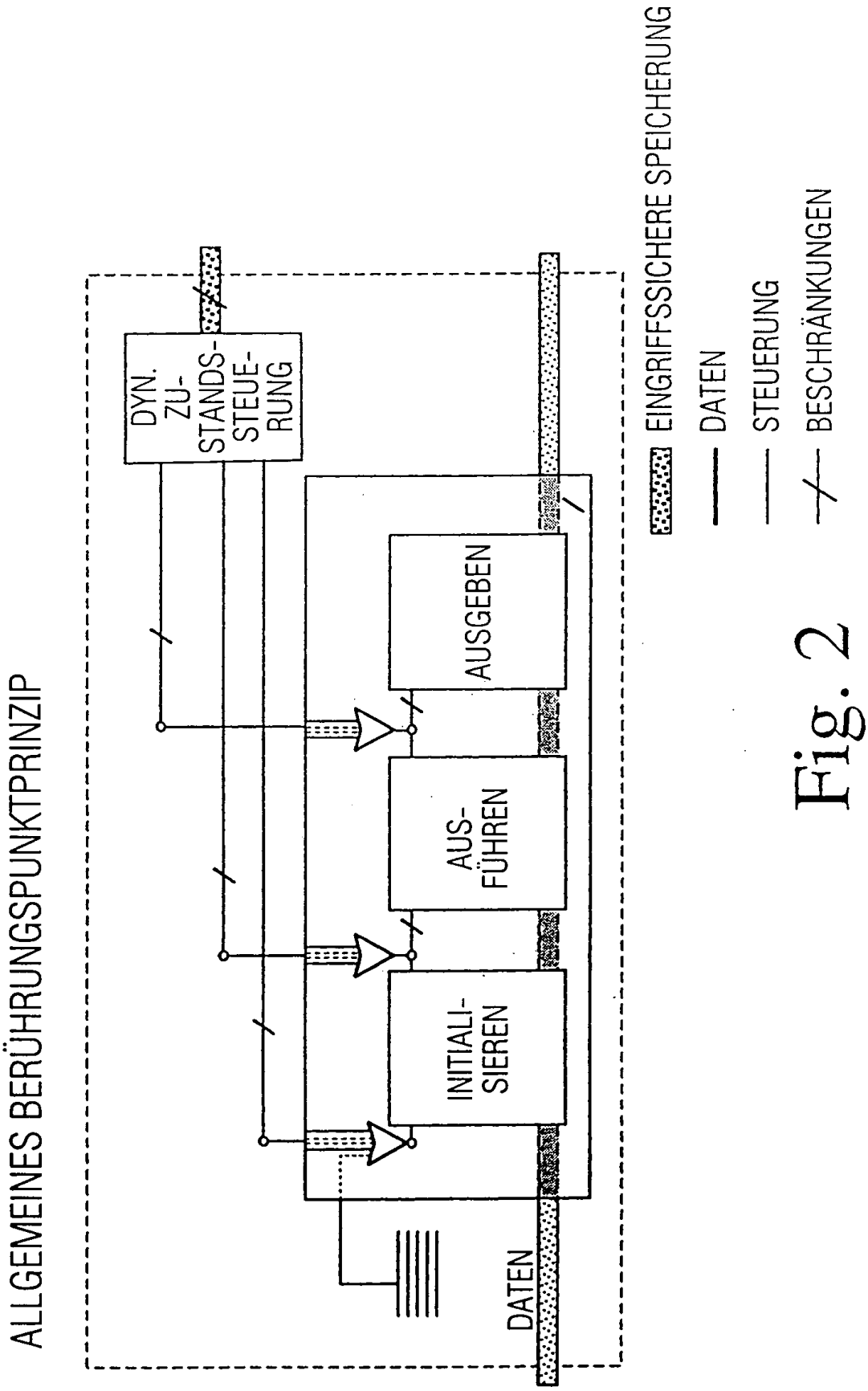

ALLGEMEINES BERÜHRUNGSPUNKTPRINZIP
DYN. ZU-STANDS-STEUE-RUNG
AUSGEBEN
AUS-FÜHREN
INITIALI-SIEREN
DATEN
EINGRIFFSSICHERE SPEICHERUNG
DATEN
STEUERUNG
BESCHRÄNKUNGEN

Fig. 2

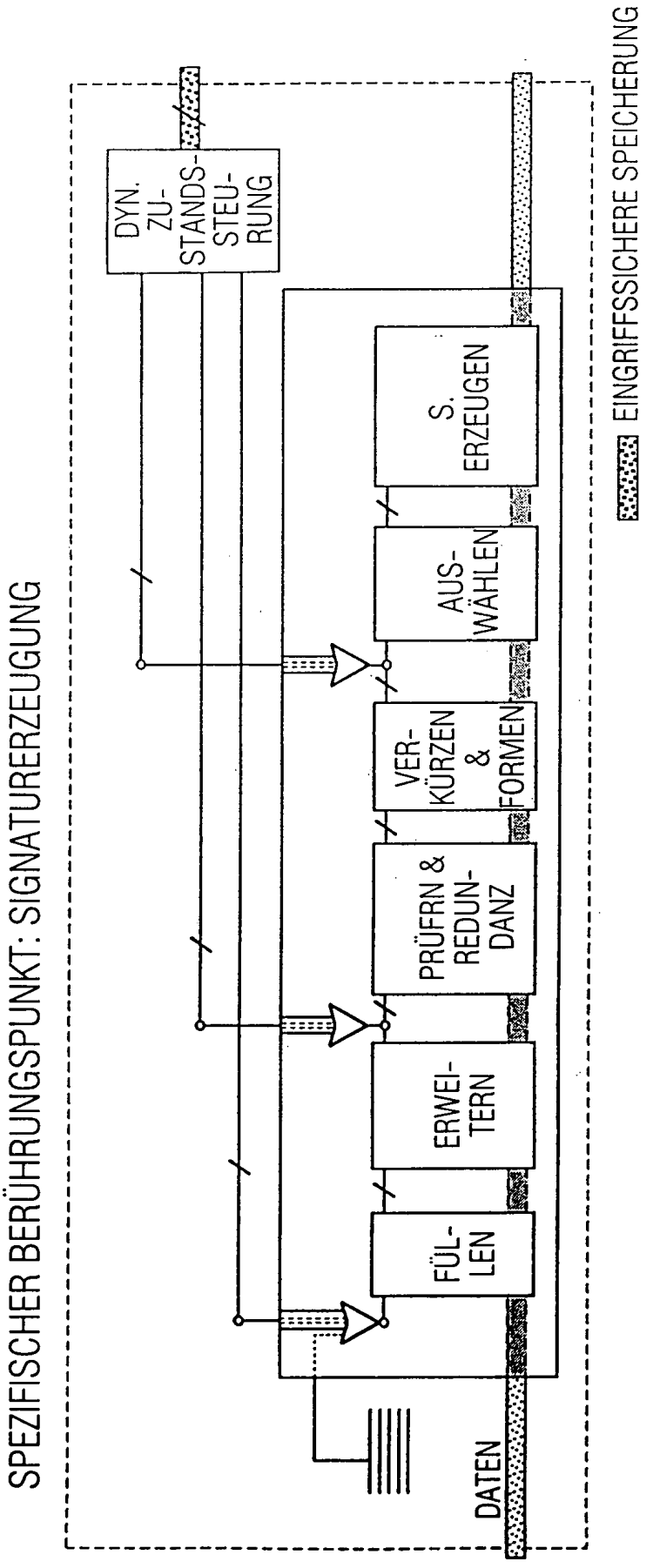

SPEZIFISCHER BERÜHRUNGSPUNKT: SIGNATURERZEUGUNG
DYN. ZU-STANDS-STEU-RUNG
S. ERZEUGEN
AUS-WÄHLEN
VER-KÜRZEN & FORMEN
PRÜFRN & REDUN-DANZ
ERWEI-TERN
FÜL-LEN
DATEN
EINGRIFFSSICHERE SPEICHERUNG
DATEN
STEUERUNG
BESCHRÄNKUNGEN

Fig. 3

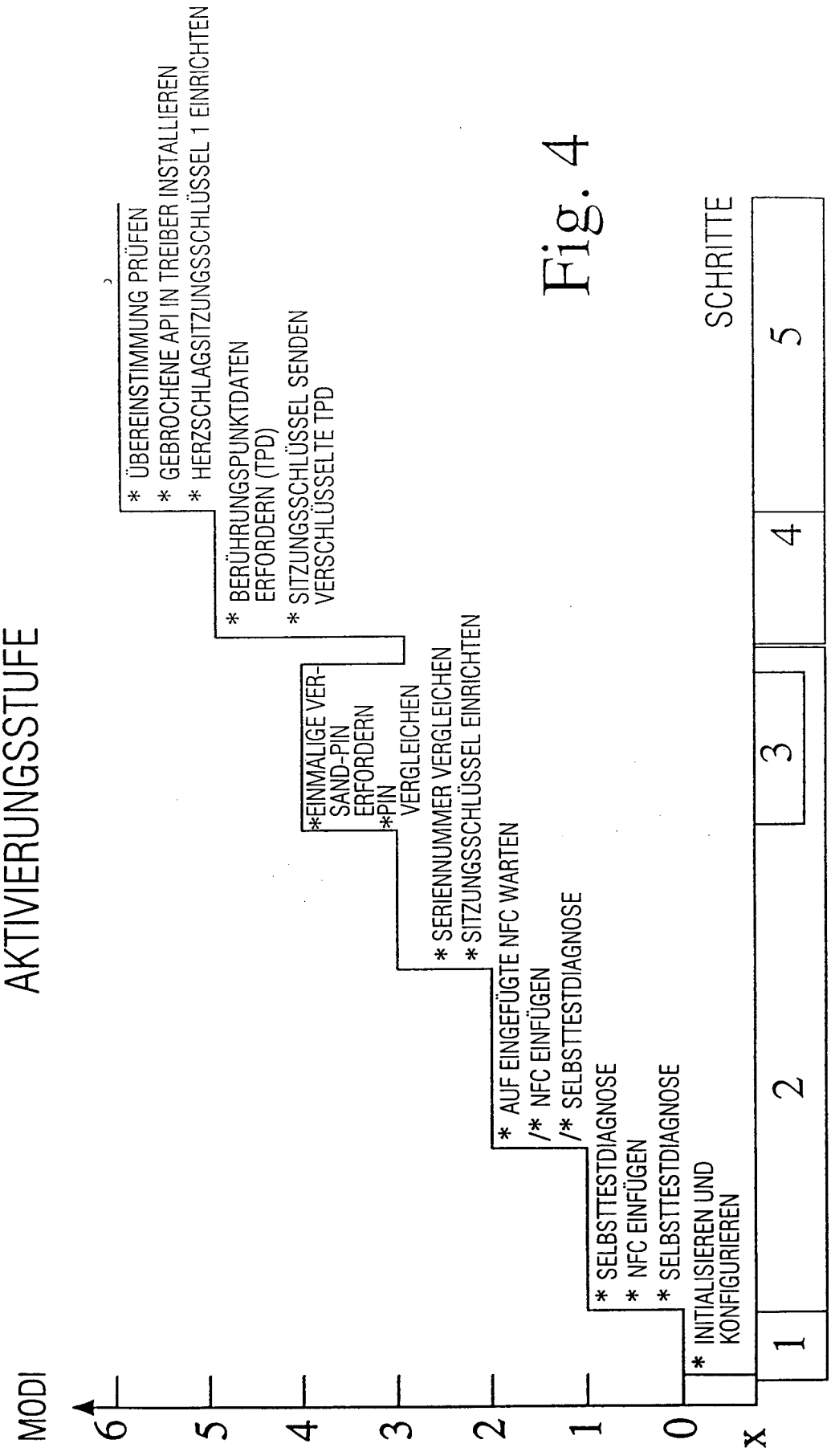

AKTIVIERUNGSSTUFE
MODI
6
5
4
3
2
1
0
x
* INITIALISIEREN UND KONFIGURIEREN
* SELBSTTESTDIAGNOSE
* NFC EINFÜGEN
* SELBSTTESTDIAGNOSE
* AUF EINGEFÜGTE NFC WARTEN
/* NFC EINFÜGEN
/* SELBSTTESTDIAGNOSE
* SERIENNUMMER VERGLEICHEN
* SITZUNGSSCHLÜSSEL EINRICHTEN
*EINMALIGE VER-SAND-PIN ERFORDERN
*PIN VERGLEICHEN
* BERÜHRUNGSPUNKTDATEN ERFORDERN (TPD)
* SITZUNGSSCHLÜSSEL SENDEN VERSCHLÜSSELTE TPD
* ÜBEREINSTIMMUNG PRÜFEN
* GEBROCHENE API IN TREIBER INSTALLIEREN
* HERZSCHLAGSITZUNGSSCHLÜSSEL 1 EINRICHTEN
1
2
3
4
5
SCHRITTE

Fig. 4

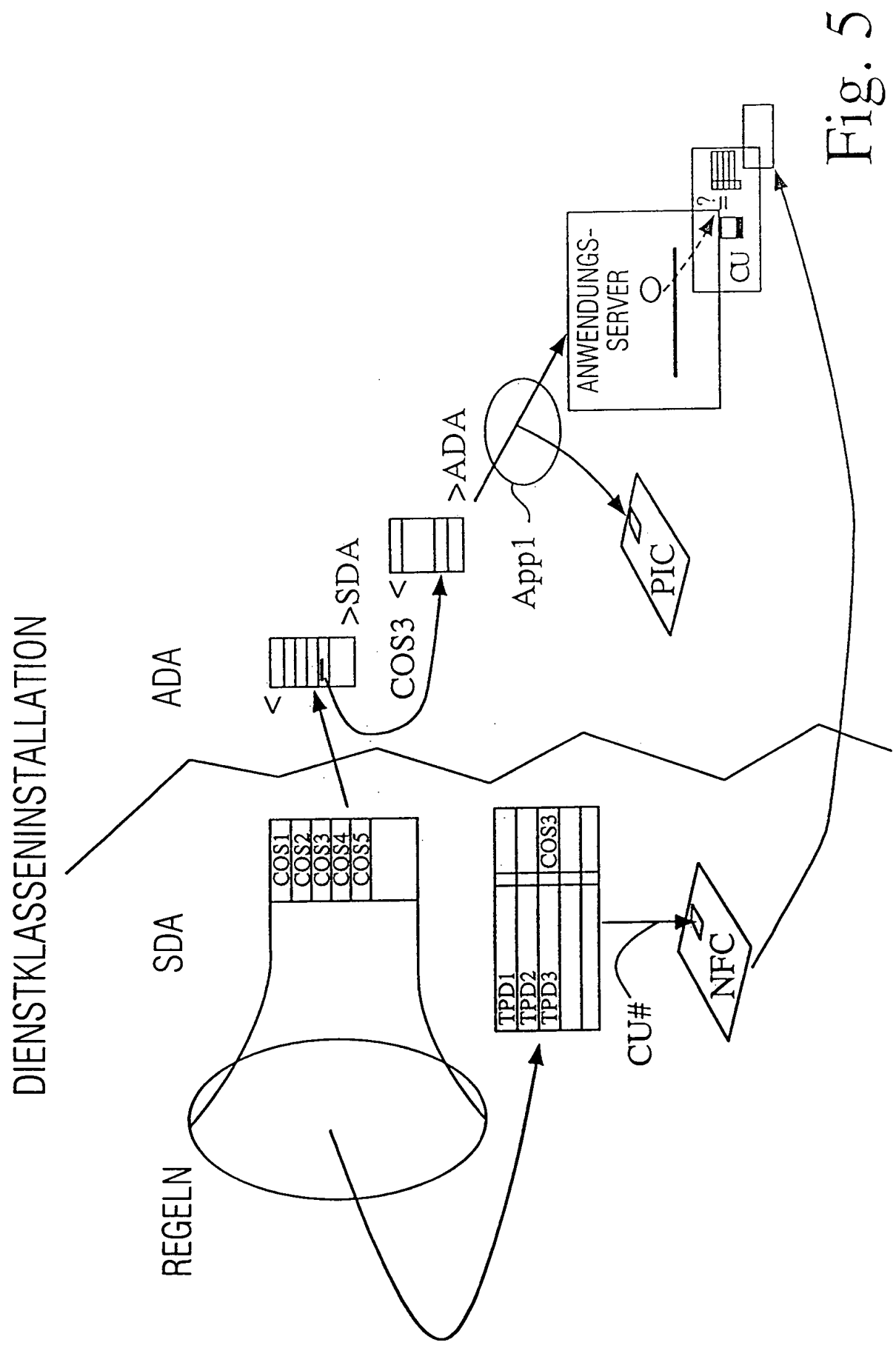

DIENSTKLASSENINSTALLATION
REGELN
SDA
ADA
COS1
COS2
COS3
COS4
COS5
<
>SDA
COS3
<
>ADA
App1
PIC
ANWENDUNGS-
SERVER
CU
TPD1
TPD2
TPD3
COS3
CU#
NFC

Fig. 5

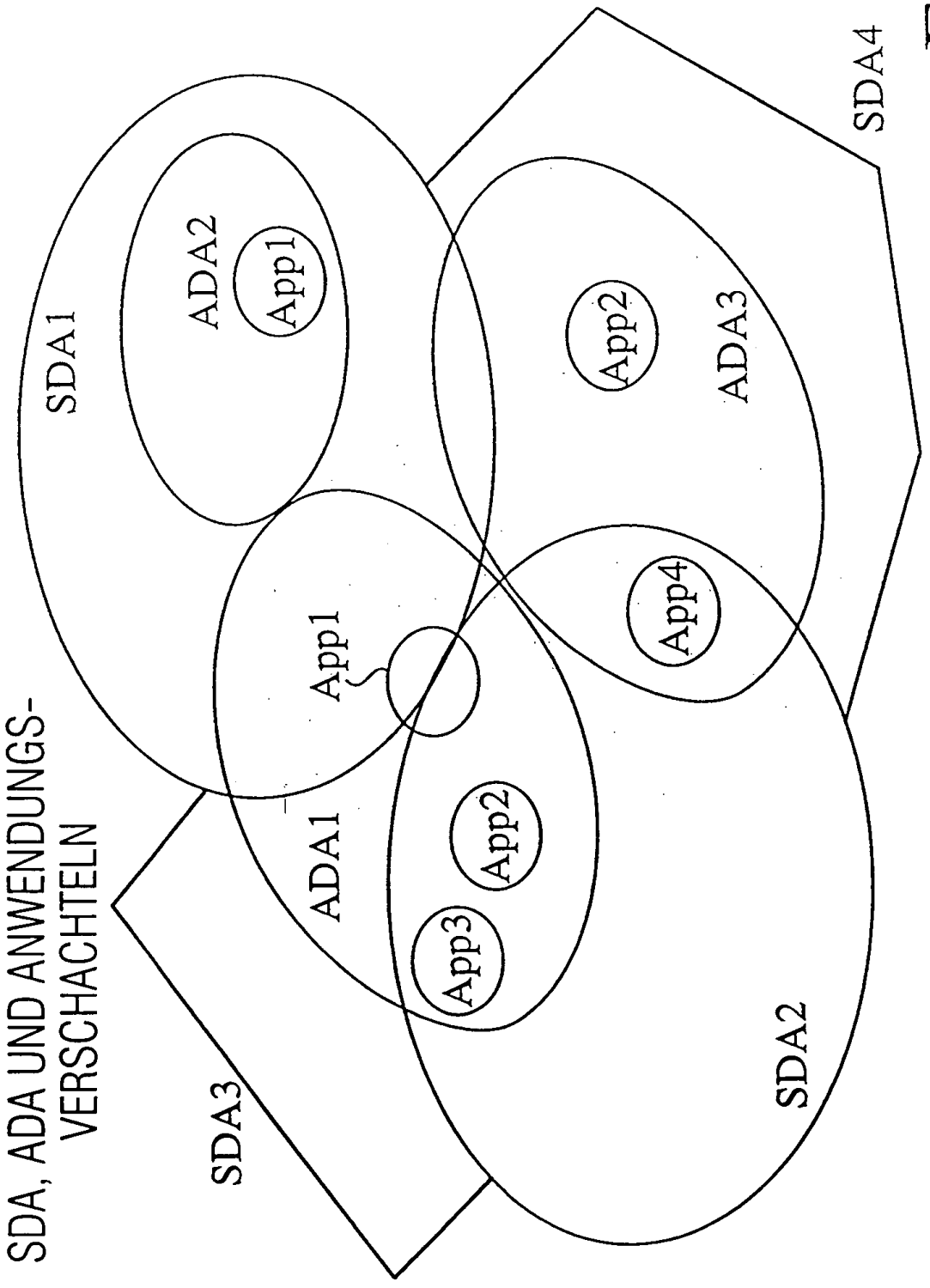

SDA, ADA UND ANWENDUNGS-VERSCHACHTELN
SDA1
ADA2
App1
SDA4
App2
ADA3
App1
App4
ADA1
App2
App3
SDA3
SDA2

Fig. 6

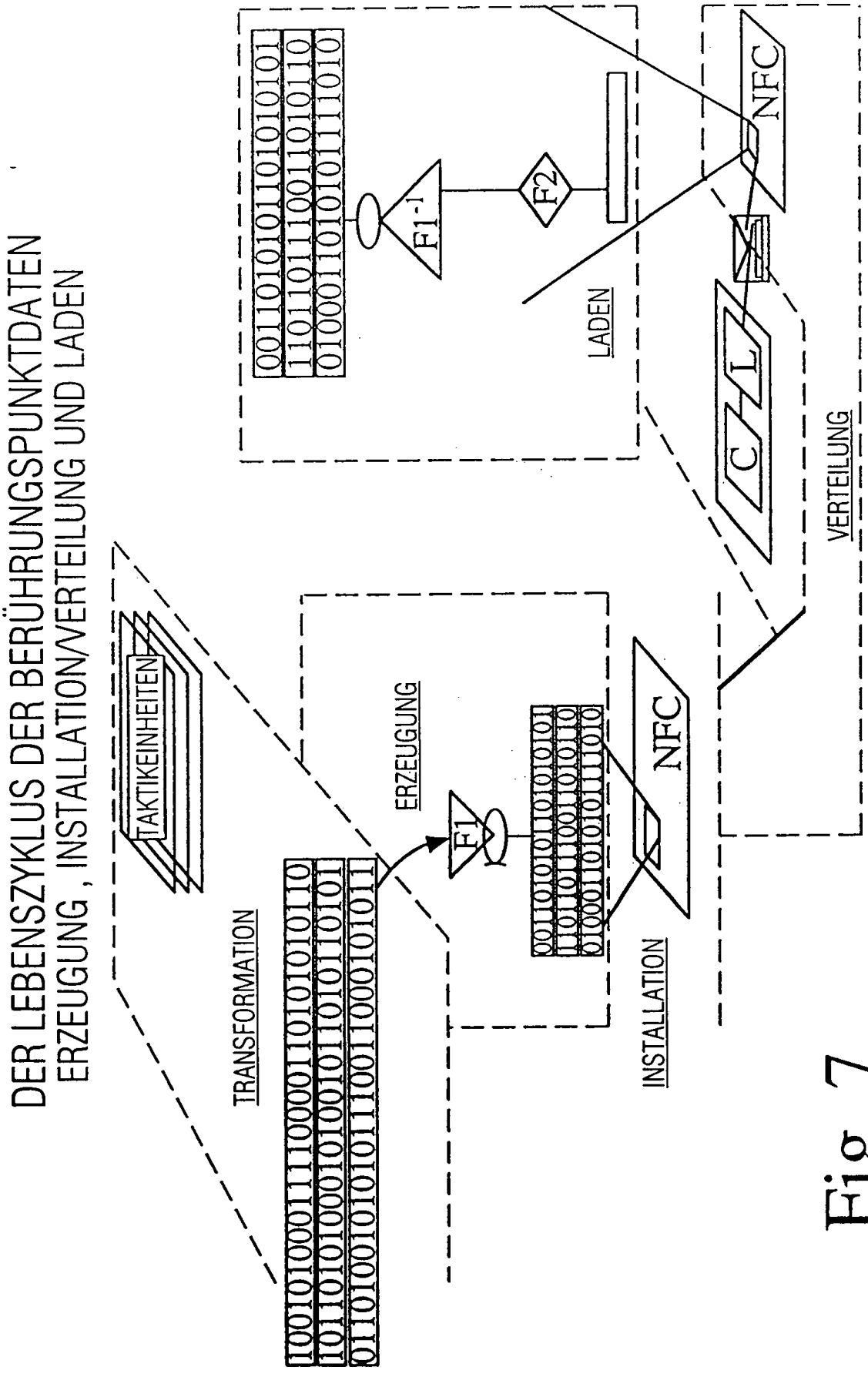

DER LEBENSZYKLUS DER BERÜHRUNGSPUNKTDATEN
ERZEUGUNG , INSTALLATION/VERTEILUNG UND LADEN
TAKTIKEINHEITEN
TRANSFORMATION
ERZEUGUNG
F1
INSTALLATION
NFC
LADEN
F1-1
F2
NFC
C
L
VERTEILUNG

Fig. 7

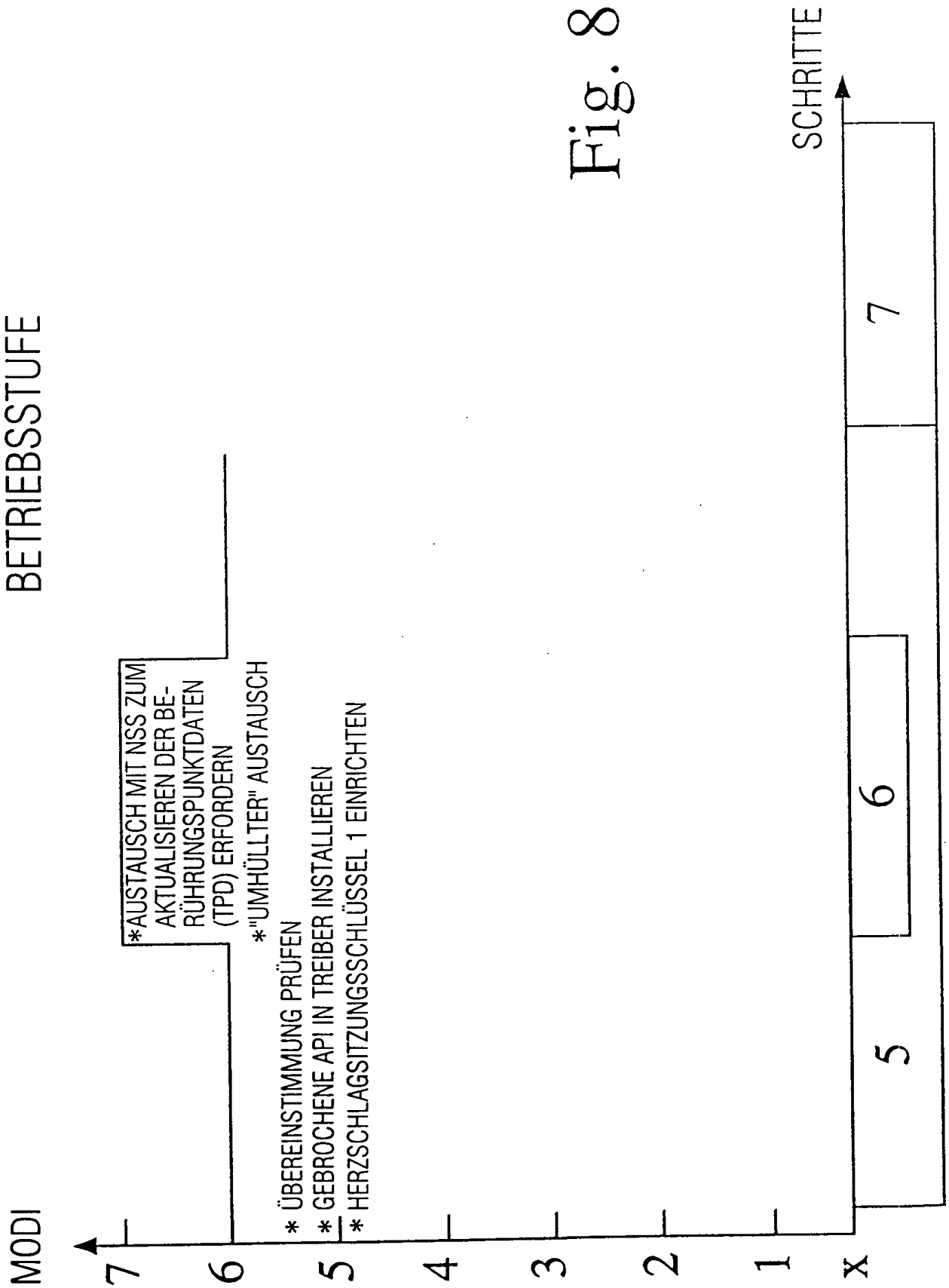
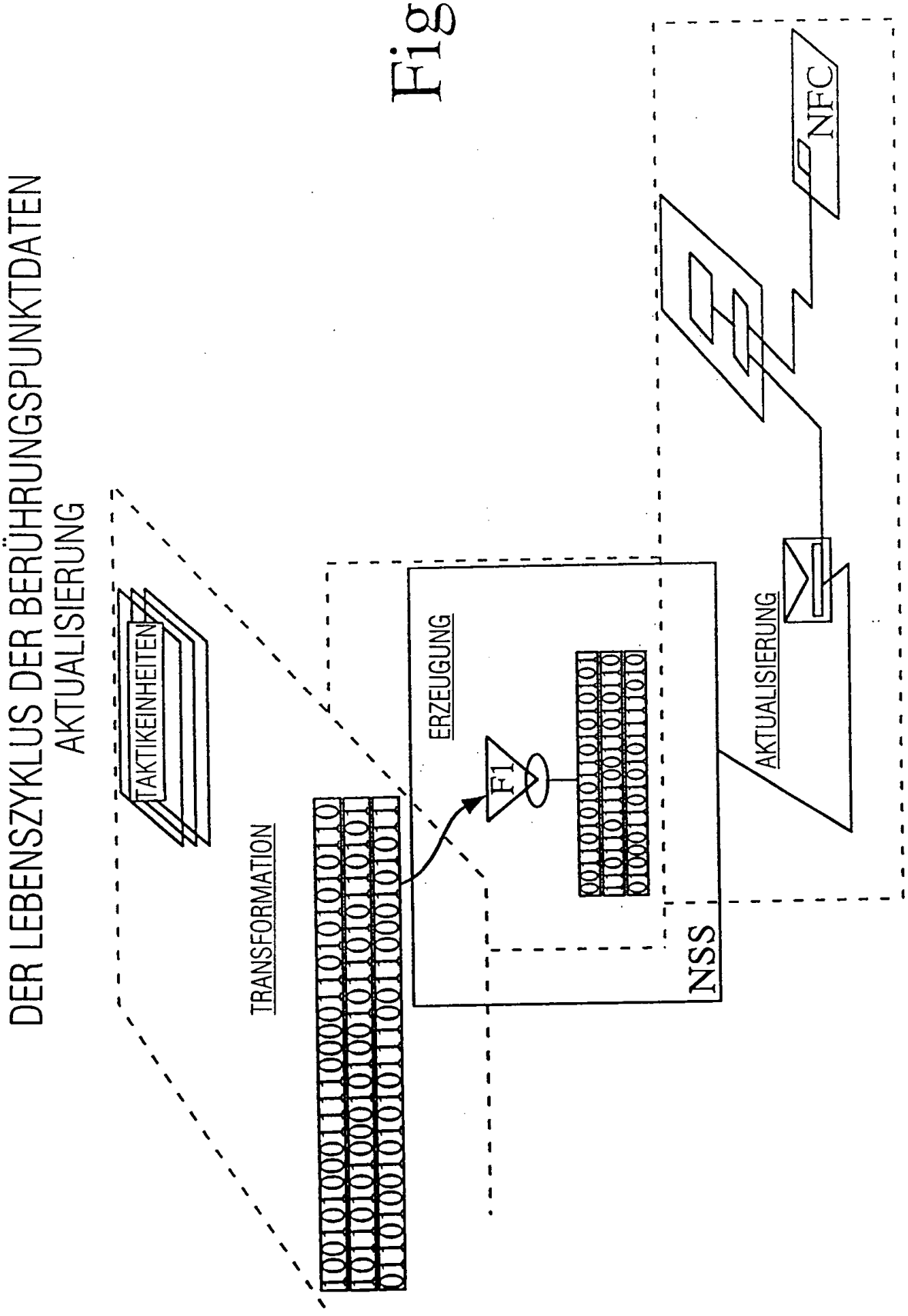

BETRIEBSSTUFE
MODI
7
6
5
4
3
2
1
x
SCHRITTE
5
6
7
*AUSTAUSCH MIT NSS ZUM AKTUALISIEREN DER BERÜHRUNGSPUNKTDATEN (TPD) ERFORDERN
*"UMHÜLLTER" AUSTAUSCH
* ÜBEREINSTIMMUNG PRÜFEN
* GEBROCHENE API IN TREIBER INSTALLIEREN
* HERZSCHLAGSITZUNGSSCHLÜSSEL 1 EINRICHTEN

Fig. 8

Fig. 9


DER LEBENSZYKLUS DER BERÜHRUNGSPUNKTDATEN
AKTUALISIERUNG
TAKTIKEINHEITEN
TRANSFORMATION
ERZEUGUNG
F1
AKTUALISIERUNG
NFC
NSS

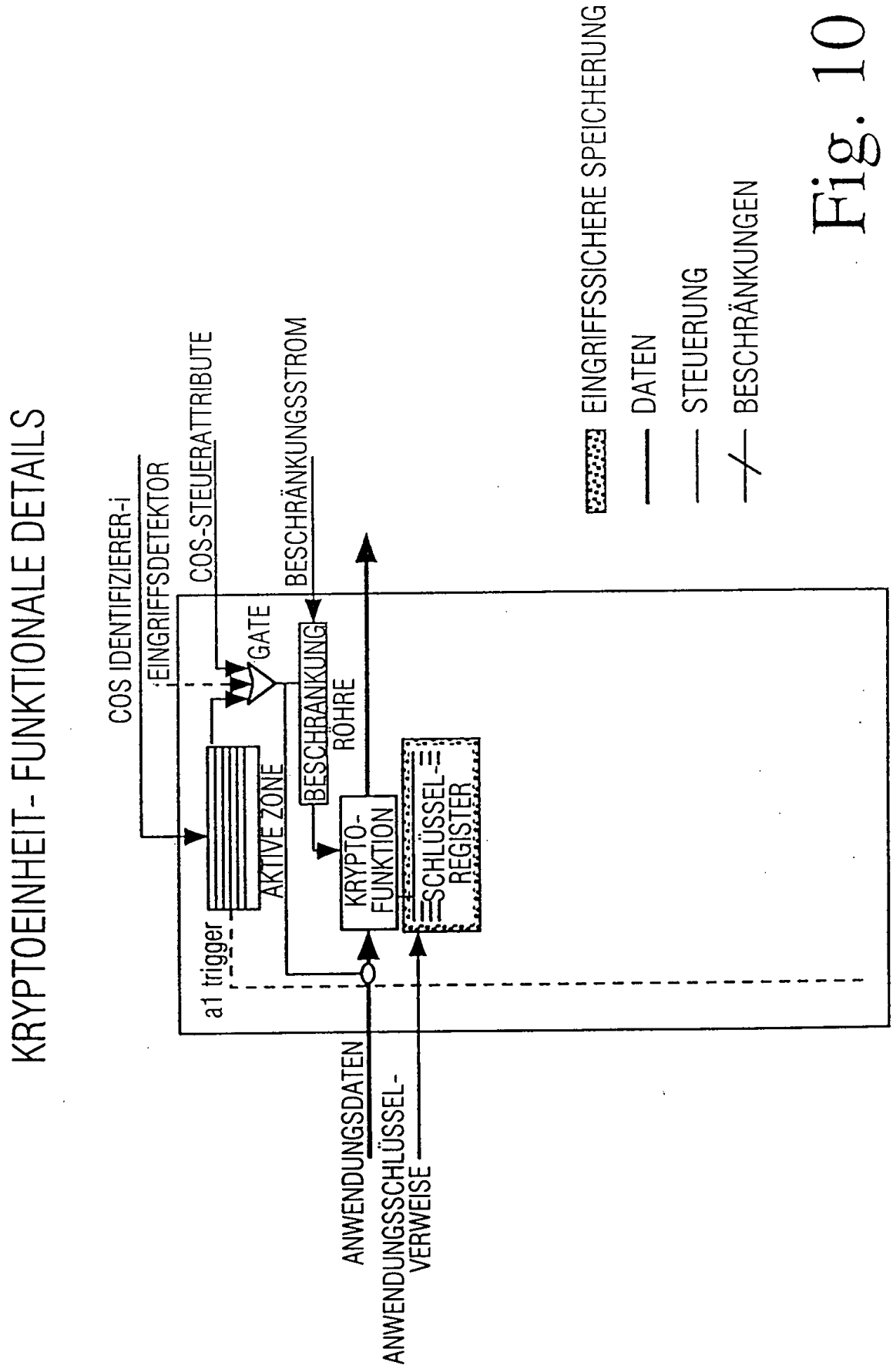

KRYPTOEINHEIT- FUNKTIONALE DETAILS
COS IDENTIFIZIERER-i
EINGRIFFSDETEKTOR
COS-STEUERATTRIBUTE
BESCHRÄNKUNGSSTROM
GATE
BESCHRÄNKUNG
RÖHRE
AKTIVE ZONE
a1 trigger
KRYPTO-
FUNKTION
SCHLÜSSEL-
REGISTER
ANWENDUNGSDATEN
ANWENDUNGSSCHLÜSSEL-
VERWEISE
EINGRIFFSSICHERE SPEICHERUNG
DATEN
STEUERUNG
BESCHRÄNKUNGEN

Fig. 10

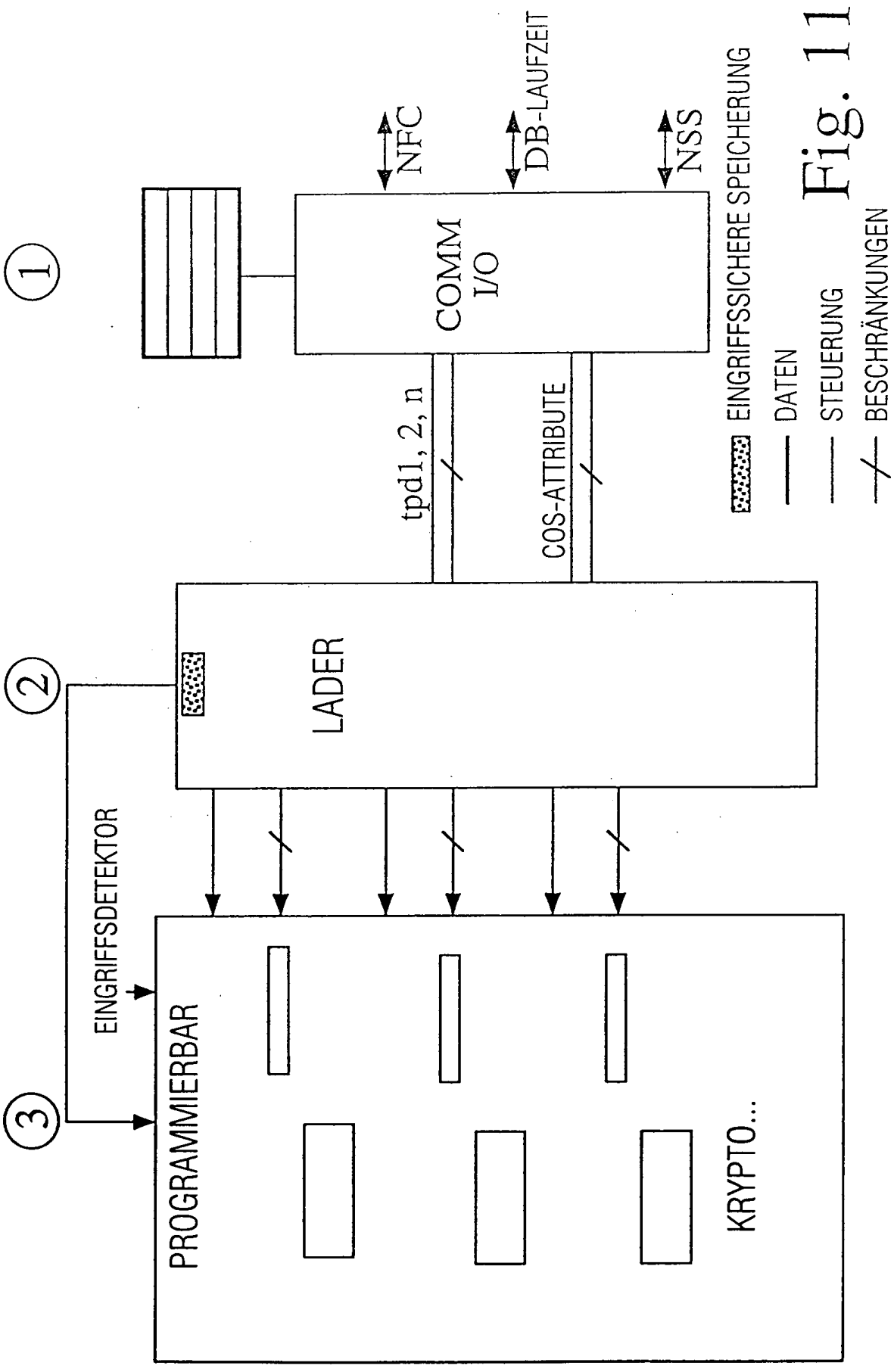

1
NFC
DB-LAUFZEIT
NSS
COMM
I/O
tpd1, 2, n
COS-ATTRIBUTE
EINGRIFFSSICHERE SPEICHERUNG
DATEN
STEUERUNG
BESCHRÄNKUNGEN
2
LADER
EINGRIFFSDETEKTOR
3
PROGRAMMIERBAR
KRYPTO...

Fig. 11

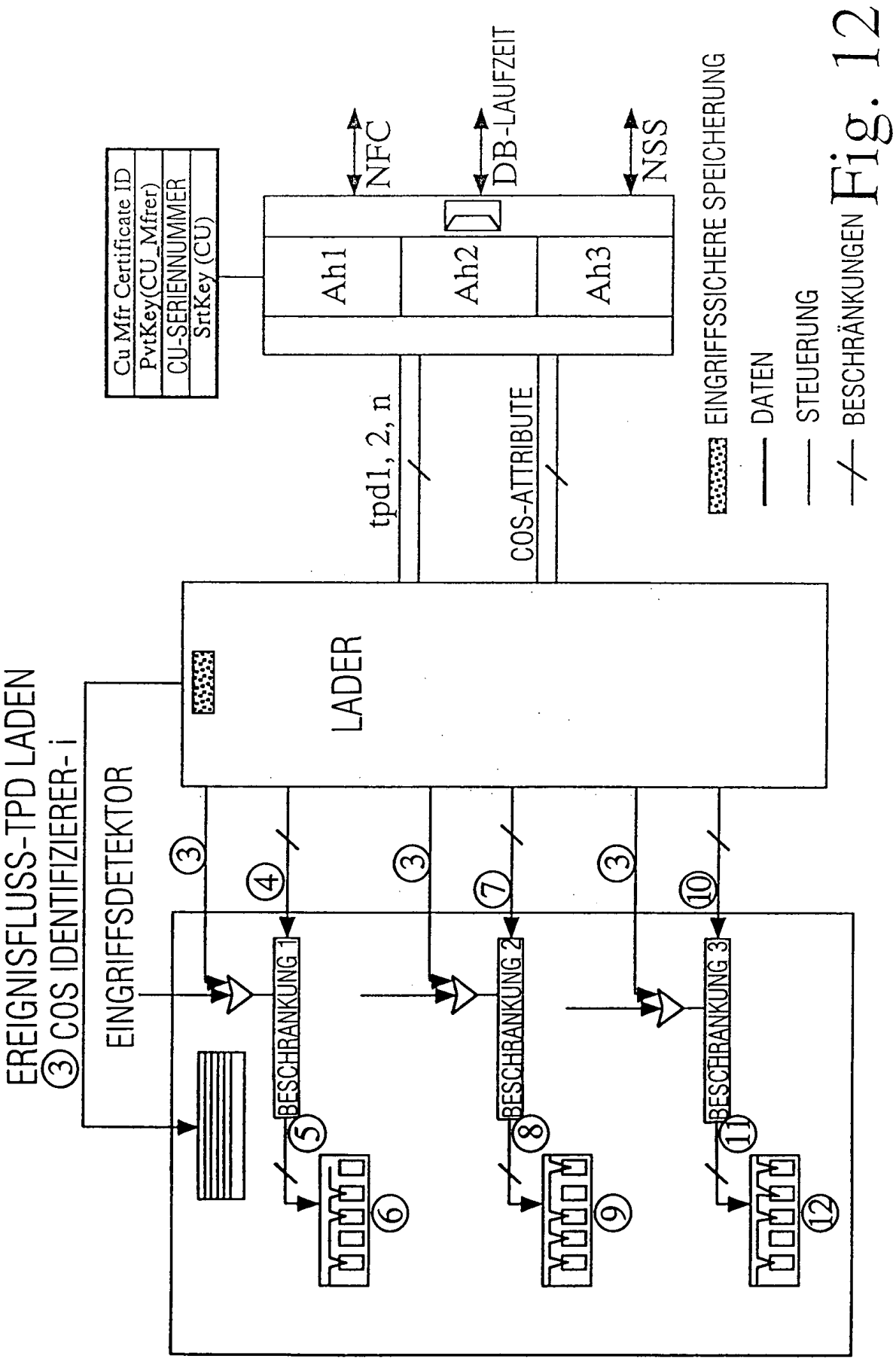

EREIGNISFLUSS-TPD LADEN
③ COS IDENTIFIZIERER- i
EINGRIFFSDETEKTOR
LADER
tpd1, 2, n
COS-ATTRIBUTE
Cu Mfr Certificate ID
PvtKey(CU_Mfrer)
CU-SERIENNUMMER
SrtKey (CU)
Ah1
Ah2
Ah3
NFC
DB-LAUFZEIT
NSS
BESCHRANKUNG 1
BESCHRANKUNG 2
BESCHRANKUNG 3
EINGRIFFSSICHERE SPEICHERUNG
DATEN
STEUERUNG
BESCHRÄNKUNGEN

Fig. 12

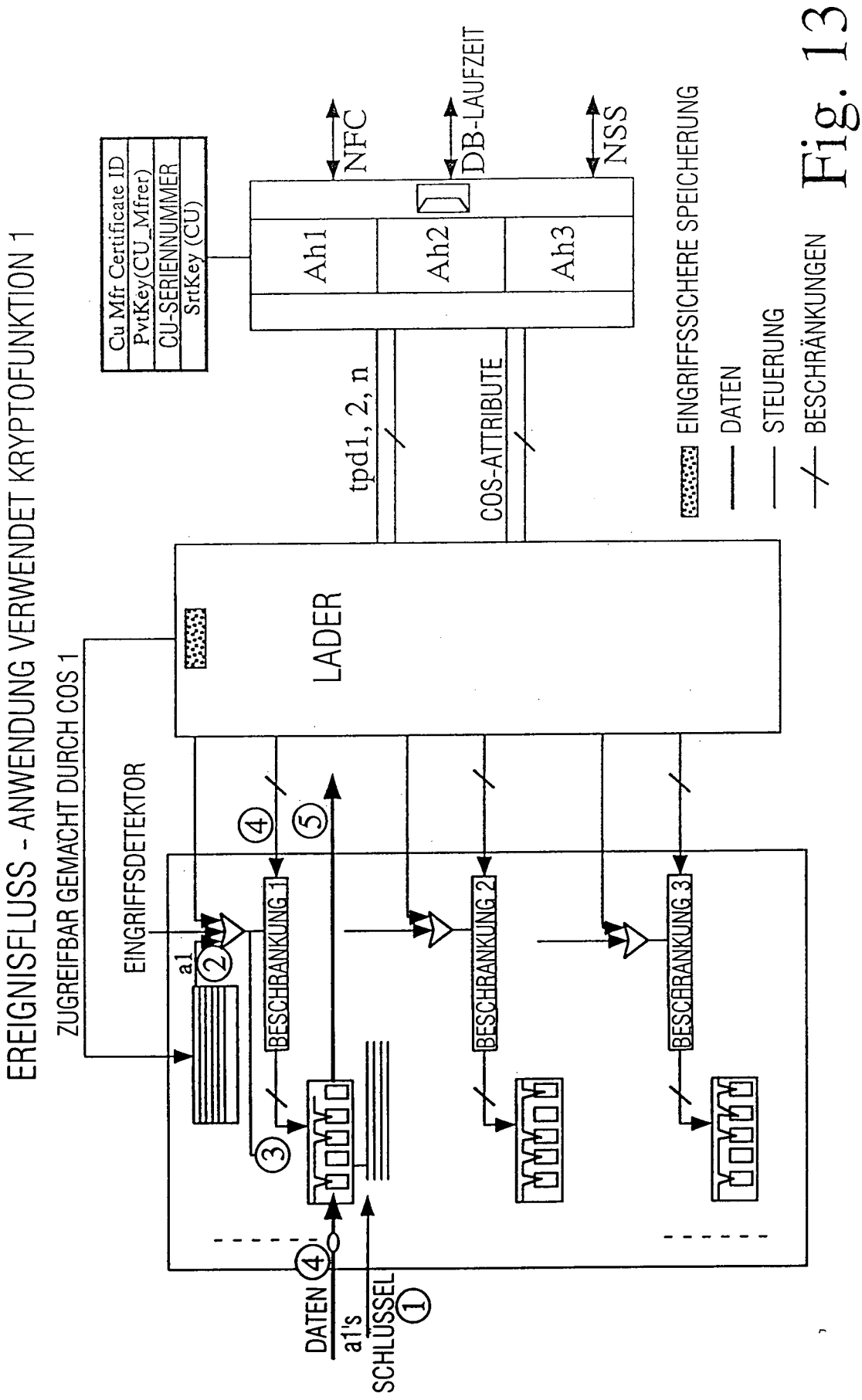

EREIGNISFLUSS - ANWENDUNG VERWENDET KRYPTOFUNKTION 1
ZUGREIFBAR GEMACHT DURCH COS 1
EINGRIFFSDETEKTOR
LADER
Cu Mfr Certificate ID
PvtKey(CU_Mfrer)
CU-SERIENNUMMER
SrtKey (CU)
Ah1
Ah2
Ah3
NFC
DB-LAUFZEIT
NSS
tpd1, 2, n
COS-ATTRIBUTE
EINGRIFFSSICHERE SPEICHERUNG
DATEN
STEUERUNG
BESCHRÄNKUNGEN
a1
BESCHRANKUNG 1
BESCHRANKUNG 2
BESCHRANKUNG 3
DATEN
a1's
SCHLÜSSEL
1
2
3
4
5

Fig. 13