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

(10) **DE 697 34 227 T2** 2006.06.29

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 0 825 512 B1**
(21) Deutsches Aktenzeichen: **697 34 227.1**
(96) Europäisches Aktenzeichen: **97 110 857.6**
(96) Europäischer Anmeldetag: **01.07.1997**
(97) Erstveröffentlichung durch das EPA: **25.02.1998**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **21.09.2005**
(47) Veröffentlichungstag im Patentblatt: **29.06.2006**

(51) Int Cl.[8]: ***G06F 21/00*** (2006.01)
H04L 9/00 (2006.01)
G06F 1/00 (2006.01)

(30) Unionspriorität:
702304 **23.08.1996** **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; Fieres, Helmut, 71126 Gäufelden, DE

(54) Bezeichnung: **Verfahren und Vorrichtung zur Erzwingung der Benutzung von Kryptographie in einer internationalen kryptographischen Struktur**

Beschreibung

[0001] Die Erfindung bezieht sich auf Kryptographie. Insbesondere bezieht sich die Erfindung auf das Inkraftsetzen einer Richtlinie, die die Verwendung von Kryptographie innerhalb des Kontexts einer internationalen Kryptographiegrundstruktur regelt.

[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.

[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 Hardwareformfaktoren, Kommunikationsprotokolle und Online- und Offline-Datendefinitionen umfassen.

[0009] Fig. 1 ist ein Blockdiagramm der internationalen Kryptographiegrundstruktur **10**, die eine Nationale-Flag-Karte **12**, eine kryptographische Einheit **14**, ein Hostsystem **16** und einen Netzwerksicherheitsserver **18** umfasst. Drei der vier Dienstelemente haben eine grundlegend hierarchische Beziehung. Die Nationale-Flag-Karte (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 wiederum das Vorliegen einer gültigen Nationale-Flag-Karte erfordert, bevor deren Dienste verfügbar sind. Das vierte Dienstelement, ein Netzwerksicherheitsserver (NSS = Network Security Server) liefert einen Bereich von unterschiedlichen Sicherheitsdiensten, einschließlich der Verifizierung der anderen drei Dienstelemente und wirkt somit als vertrauenswürdiger Dritter.

[0010] Fig. 2 ist eine perspektivische Ansicht, die die vier Grundelemente der Grundstruktur zeigt, einschließlich der kryptographischen Einheit **14** und mehrerer Nationale-Flag-Karten **12**, eines Hostsystems **16** und eines nationalen Sicherheitsservers **18**. In den folgenden Abschnitten wird jedes Dienstelement näher erörtert.

[0011] Nationale-Flag-Karte (NFC). Bei einem Ausführungsbeispiel ist die NFC **12** eine kleine, briefmarkengroße (25 × 15 mm) ISO 7816-Typ Smartcard, d. h. ein Ein-Chip-Computer **26** mit einem nichtflüchtigen Speicher. Die NFC ist auf einem starren Substrat befestigt und in einer eingriffsicheren Verpackung abgedichtet. Die NFC wird typischerweise durch nationale Behörden unabhängig erzeugt und verteilt (z. B. United States Postal Service, Deutsche Bundespost). Nationale Behörden können auch an private Industrien eine Lizenz für die NFC-Herstellung und Verteilung erteilen.

[0012] Die Wirkung des NFC-Dienstelements ist es, eine Richtlinie eines Landes geltend zu machen, die die Verwendung von Kryptographie regelt. Eine NFC ist ein vollständiger Computer, der als eine Mehrchiparchitektur aufgebaut werden kann, um kundenspezifische integrierte Schaltungen zu umfassen. Dieselbe würde außerdem eingriffssichere und eindeutige Identifikationsmerkmale umfassen, die einen unbefugten Eingriff oder Duplizierung unmöglich machen. Beispielsweise könnte die NFC auf solche Weise abgedichtet sein, dass das Öffnen der Verpackung derselben jede integrierte Schaltung oder Daten in derselben zerstören würde. Die NFC könnte den Empfang einer verschlüsselten Autorisierung erfordern, die durch den nationalen Sicherheitsserver ausgegeben wird. Alle Dienste der NFC werden über ein Standard-ISO-7816-Mitteilungsaustauschprotokoll zwischen der NFC und anderen Dienstelementen geliefert. Dieses Format ist identisch mit der Smartcard, die in Europa verwendet wird, um GSM in Mobilsprachdiensten zu unterstützen.

[0013] Kryptographische Einheit (CU). Die kryptographische Einheit ist eine eingriffssichere Hardwarekomponente, die entworfen ist, um geschützte kryptographische Dienste unter der strengen Kontrolle einer NFC zu liefern. Kryptographische Einheiten werden konkurrierend von Systemverkäufern und von Dritten hergestellt und sind frei von Import- und Exportbeschränkungen. Weil die kryptographische Einheit kritische Sicherheitselemente umfasst, wie z. B. Verschlüsselungsalgorithmen und Schlüssel, ist es wahrscheinlich, dass dieselbe für eine Kundengarantie zertifiziert ist (z. B. NIST-, NCSC- oder ITSEC-zertifiziert). Es ist ein Merkmal dieses Ausführungsbeispiels der Erfindung, dass die kryptographische Einheit keine andere bestimmende Richtlinie enthält außer ihrer Abhängigkeit von einer NFC. Diese Komponente ist vorzugsweise für eine Leistung und Schutz mit einer Kundeneinstellung für ein bestimmtes Hostsystem entworfen.

[0014] Hostsystem (HS). Das HS ist als die Hardwarekomponente identifizierbar, die sichere Informationstechnologiedienste direkt an den Benutzer liefert. Ein HS ist typischerweise ein Universalinformationstechnologiegerät und wird konkurrierend in einem breiten offenen Markt hergestellt. Beispiele umfassen Personaldigitalassistenten, Personalcomputer, Workstations, Laptops, Palmtops, vernetzte Server, Großcomputer, Netzwerkdrucker oder Videoanzeigeeinheiten, und auch eingebettete Systeme für Steuerung und Messung. Die Funktion des HS-Dienstelements in der Grundstruktur ist es, eine Anwendungsprogrammierschnittstelle (API) zum Zugreifen auf das Kryptographische-Einheit-Dienstelement zu liefern. Kryptographische-Einheit-Unterstützung wird vorzugsweise als eine Option geliefert, die auf dem HS verfügbar ist.

[0015] Netzwerksicherheitsserver (NSS). Der NSS ist ein Netzwerkknoten, der entworfen und bestimmt ist, um vertrauenswürdige dritte Sicherheitsdienste zu liefern. Beispielsweise muss jeder Netzwerkzugriff, wie z. B. über Modems **30**, **32** über eine Netzwerk **34** durch den NSS identifiziert werden. Im Zusammenhang nationaler Sicherheit werden NSS vorzugsweise von Regierungsbehörden entwickelt und betrieben und gehören denselben. Einige der Funktionen, die durch das NSS-Dienstelement geliefert werden, umfassen Dienstelementauthentifizierung, Mitteilungsstempelauthentifizierung, in Kraft setzen nationaler Richtlinien und Verteilung kryptographischer Schlüssel. Die Wichtigkeit des NSS kann sich in Umgebungen stark erhöhen, wo ein hoher Grad an Verifizierung eine Voraussetzung für kryptographische Verwendung ist. Der NSS spielt auch eine wesentliche Rolle bei der Interoperabilität von unter-

schiedlichen nationalen kryptographischen Richtlinien bzw. Taktiken.

[0016] Schutzbereich oder Umfang der Grundstruktur. Der Schutzbereich der Grundstruktur ist überwiegend definiert durch den Schutzbereich der NFCs. Der Grundschutzbereich der NFCs ist der einer Domain bzw. eines Bereichs. Eine Domain kann so groß sein wie weltweit und so klein wie eine Firmeneinheit. Auf der Domainebene gibt es keine eindeutige Unterscheidung zwischen ihren Mitgliedern. Obwohl sich diese Grundstruktur hauptsächlich auf nationale und internationale Domains konzentriert (z. B. Frankreich, Deutschland, Vereinigte Staaten, Großbritannien, Europäische Gemeinschaft, Nato, Nordamerika, G7), werden andere Domains oder Subdomains ebenfalls in Betracht gezogen. Beispielsweise Industriedomains (z. B. Telekommunikation, Gesundheitsvorsorge, Finanzdienste, Reisen), Firmendomains (z. B. Hewlett Packard, Ford Motor Company, CitiBank), Vereinigungsdomains (z. B. IEEE, ISO, X/Open), Dienstleisterdomains (z. B. Compuserve, America On-Line) und Produktdomains (z. B. Lotus, Microsoft, General Motors, Proctor & Gamble).

[0017] Über Domains und Subdomains hinaus kann der Schutzbereich der Grundstruktur optional ausgedehnt werden, um die Eindeutigkeit in einer Domains zu definieren. Erneut sind es die NFCs, die diesen engeren Schutzbereich möglich machen. Das Bereitstellen einer Eindeutigkeit bedeutet das Ermöglichen, dass die Übertragung eindeutiger oder persönlicher Daten an die NFC erlaubt wird, entweder zum Zeitpunkt des Kaufs oder zum Zeitpunkt der anfänglichen Validierung. NFCs werden als anonym angesehen, wenn sie auf der Domainebene arbeiten. Wenn eine Eindeutigkeit hinzugefügt wird, sind NFCs nicht mehr anonym.

[0018] Verbinden von Grundstrukturelementen. Die Verbindung von Dienstelementen (z. B. NFC, kryptographische Einheit, HS, NSS) dieser Grundstruktur wird durch die Annahme von Standardanwendungsprogrammschnittstellen- (z. B. X/Open, OSF) und Industriestandardprotokoll-Austausch (z. B. TCP/IP, ISO, DCE, X.509) erreicht. Die Verbindung von Elementen kann synchron sein (d. h. online), asynchron (d. h. offline), lokal (z. B. Laufzeitbibliothek) entfernt (z. B. RPC), oder jede Kombination derselben. Beispielsweise könnte eine Richtlinie, die die Personalisierung von NFCs umfasst, eine einmalige Autorisierungsfunktion über ein NSS durchführen, was eine zukünftige Onlineverifizierung mit einem NSS unnötig macht, bis die NFC abläuft.

[0019] Über die physikalische Verbindung der Dienstelemente der Grundstruktur hinaus geht der Mitteilungsaustausch zwischen den Elementen und den tatsächlichen Diensten, die über diesen Mitteilungsaustausch geliefert und angefordert werden. Fig. 3 stellt die Mitteilungsaustauschwege zwischen einer NFC **12** und einer kryptographischen Einheit **14** (Weg **35**), zwischen der kryptographischen Einheit **14** und einem HS **16** (Weg **36**) und zwischen dem HS **16** und einem NSS **18** (Weg **37**) dar. Eine virtuelle Verbindung **38** besteht zwischen der NFC und dem NSS. Das Mitteilungsübermittlungsprotokoll zwischen dem HS und der kryptographischen Einheit entlang dem Weg **36** wird am besten von kryptographischen API-Standardisierungsbemühungen (z. B. kryptographische API von NSA, kryptographische API von Microsoft) entnommen. Das Mitteilungsübermittlungsprotokoll zwischen der kryptographischen Einheit und der NFC entlang dem Weg **35** ist in zwei Gruppen unterteilt: Initialisierungsprotokolle und Betriebsprotokolle. Die Initialisierungsprotokolle müssen erfolgreich sein, bevor Betriebsprotokolle aktiv sind.

[0020] Kritisch für die Implementierung der Grundstruktur ist die Bereitstellung einer grundlegenden Technologie, die die Herstellung der verschiedenen Dienstelemente ermöglicht. Obwohl verschiedene Implementierungen 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.

[0021] Folglich wäre es sinnvoll, eine gemeinsame akzeptierte Kryptographiegrundstruktur zu schaffen, bei der unabhängige Technologie- und Taktikauswahlen auf eine Weise getroffen werden können, die nach wie vor eine internationale Kryptographiekommunikation ermöglicht, die mit diesen Richtlinien übereinstimmt. Ferner wäre es sinnvoll, verschiedene Konfigurationen zu schaffen, die Flexibilität bei der Implementierung einer solchen Kryptographiegrundstruktur ermöglichen, ohne die Sicherheit und Steuerung zu beeinträchtigen, die durch eine solche Grundstruktur gewährt werden, insbesondere wenn die Richtlinie, die in der Grundstruktur in Kraft gesetzt wurde, in einer der mehreren unterschiedlichen Konfigurationen verfügbar war.

[0022] Die EP-A-0731406, die nach dem Prioritätsdatum der vorliegenden Anmeldung veröffentlicht wurde und daher gemäß Artikel 54 (3) EPÜ Stand der Technik bildet, bezieht sich auf eine internationale Kryptographiegrundstruktur, die eine National-Flag-Karte, die angepasst ist, um zumindest einen definierenden Parameter eines Verschlüsselungsschemas unterzubringen, das durch eine bestimmte nationale Richtlinie gefordert wird, eine kryptographische Einheit, die angepasst ist, um das Verschlüsselungsschema zu implementieren, falls die kryptographische Einheit in Kombination mit der nationalen Flag-Karte verwendet wird, und ein Hostsystem umfasst, das für die Kommunikation mit der kryptographischen Einheit angeordnet ist und angepasst ist, um das Verschlüsselungsschema zu implementie-

ren, falls und nur falls das Hostsystem in Kombination mit einer kryptographischen Einheit und einer gültigen nationalen Flag-Karte verwendet wird.

[0023] Die US-A-5164988 bezieht sich auf ein verteiltes System, bei dem ein erster Datenprozessor, dem ein erstes kryptographisches System zugeordnet ist, eine Netzwerksicherheitsrichtlinie in einem ersten Konfigurationsvektor codiert. Der erste Konfigurationsvektor wird an einen zweiten Datenprozessor übertragen, dem ein zweites kryptographisches System zugeordnet ist, wobei der zweite Datenprozessor gemäß dem ersten Konfigurationsvektor konfiguriert ist, um die Netzwerksicherheitsrichtlinie zu implementieren.

[0024] Ferreira R. „The Practical Application of State of the Art Security in Real Environments", Advances in Cryptology – Auscrypt '90, 8. Januar 1990, Sydney, Australien, Seiten 334 bis 355, bezieht sich auf eine Implementierung von Sicherheit in realen Umgebungen und bezieht sich auf die Verwendung verschiedener Kartentypen, die für anwendungsspezifische Zwecke in einer Sicherheitsumgebung geliefert werden. Verschiedene Kartentypen werden offenbart zum Bereitstellen unterschiedlicher Authentifizierungsebenen für unterschiedliche Bedienpersonen.

[0025] Es ist die Aufgabe der vorliegenden Erfindung, eine sichere Kryptographiegrundstruktur zu schaffen, in der eine Anzahl von kryptographischen Einheiten unter Verwendung einer einzigen Richtlinienkarte sicher gesteuert werden können, die ein kryptographisches Schema für die kryptographischen Einheiten enthält.

[0026] Diese Aufgabe wird durch eine kryptographische Grundstruktur gemäß Anspruch 1 gelöst.

[0027] Die Erfindung schafft ein flexibles Richtlinienelement, das verschieden konfiguriert werden kann, für gewählte Anwendungen, die eine Vier-Teil-Technologiegrundstruktur verwenden, die internationale Kryptographie unterstützt. Die Kryptographiegrundstruktur umfasst die Richtlinie, d. h. eine Nationale-Flag-Karte (NFC), eine kryptographische Einheit, ein Hostsystem und einen Netzwerksicherheitsserver. Drei der vier Dienstelemente haben eine im Wesentlichen hierarchische Beziehung. Die Nationale-Flag-Karte (NFC), die hierin auch als die „Richtlinie" bezeichnet wird, wird in die kryptographische Einheit (CU) installiert, die wiederum in ein Hostsystem (HS) installiert ist. Kryptographische Funktionen auf dem Hostsystem können nicht ohne eine kryptographische Einheit ausgeführt werden, die selbst das Vorliegen einer gültigen Nationale-Flag-Karte erfordert, bevor die Dienste derselben verfügbar werden. Das vierte Dienstelement, ein Netzwerksicherheitsserver (NSS) kann eine Reihe unterschiedlicher Sicherheitsdienste liefern, einschließlich der Verifizierung der anderen drei Dienstelemente.

[0028] Die Erfindung spezifiziert mehrere unterschiedliche Konfigurationen, die eine Richtlinie in einem kryptographischen System unterstützen, wie z. B. die internationale Kryptographiegrundstruktur. Solche Konfigurationen liefern beträchtliche Flexibilität, die es der Grundstruktur ermöglicht, an verschiedene Verbindungsschemen angepasst zu werden, die zumindest die kryptographische Einheit und die Richtlinie umfassen. Bei allen Ausführungsbeispielen der Erfindung ist es ein steuerndes Prinzip, dass die Kryptographie bei Abwesenheit einer Richtlinie einem Benutzer der kryptographischen Einheit nicht verfügbar gemacht wird.

[0029] Die Erfindung liefert auch verschiedene Verbesserungen bei der Interoperabilität und ermöglicht die Koexistenz unterschiedlicher Konfigurationen. Bei dem beispielhaften Ausführungsbeispiel der Erfindung umfassen solche Konfigurationen zweckgebundene Anwendungen, z. B. eine Richtlinie, die in einer kryptographischen Einheit vorgesehen ist, die entweder einen eingebauten oder lokalen Smartcardleser aufweist, oder eine Richtlinie in einem entfernten Smartcardleser; und gemeinschaftlich verwendete Anwendungen, z. B. eine Richtlinie, die in einem lokalen Smartcardleser eines Hostsystems vorgesehen ist.

[0030] Fig. 1 ist ein Blockdiagramm einer internationalen Kryptographiegrundstruktur, die eine nationale Flagkarte, eine kryptographische Einheit, ein Hostsystem und einen Netzwerksicherheitsserver umfasst;

[0031] Fig. 2 ist eine schematische Darstellung, die ein allgemeines Berührungspunktprinzip gemäß der Erfindung zeigt;

[0032] Fig. 3 ist eine schematische Darstellung, die einen spezifischen Berührungspunkt zeigt, der eine Signaturerzeugung gemäß der Erfindung liefert;

[0033] **Fig.** 4a ist eine schematische Darstellung, die physikalische und logische Verbindungsendpunkte der vier Grundstrukturdienstelemente in einer nicht vertrauenswürdigen Umgebung darstellt;

[0034] Fig. 4b ist eine schematische Darstellung, die physikalische und logische Verbindungsendpunkte der vier Grundstrukturdienstelemente in einer vertrauenswürdigen Umgebung darstellt;

[0035] Fig. 5a sind schematische Blockdiagramme, die die n-äre bis Fig. 5f Beziehungen zwischen den Grundstrukturelementen durch Verbindungsendpunkte darstellen, die zwischen einer Richtlinie und

einer kryptographischen Einheit hergestellt sind; und

[0036] Fig. 6a sind schematische Blockdiagramme, die die n-äre bis Fig. 6f Beziehungen zwischen den Grundstrukturelementen durch Verbindungsendpunkte darstellen, die zwischen einer Richtlinie und einem NSS hergestellt sind;

[0037] Fig. 7a liefern ein schematisches Blockdiagramm eines bis Fig. 7c zweckgebundenen Richtlinienelements gemäß drei alternativen Anordnungen eines ersten bevorzugten Ausführungsbeispiels der Erfindung;

[0038] Fig. 8 ist ein schematisches Blockdiagramm eines weiteren zweckgebundenen Richtlinienelements gemäß einem zweiten bevorzugten Ausführungsbeispiel der Erfindung;

[0039] Fig. 9 ist ein schematisches Blockdiagramm eines gemeinschaftlich verwendeten Richtlinienelements gemäß einem dritten bevorzugten Ausführungsbeispiel der Erfindung; und

[0040] Fig. 10 ist ein schematisches Blockdiagramm eines weiteren zweckgebundenen Richtlinienelements gemäß einem vierten bevorzugten Ausführungsbeispiel der Erfindung.

Detaillierte Beschreibung der Erfindung

[0041] Eine nationale Kryptographierichtlinie variiert häufig nach Industriesegment, politischem Klima und/oder Mitteilungsfunktion. Dies macht es schwierig, allen Industrien für alle Zeiten eine einheitliche Richtlinie bzw. Taktik zuzuweisen, folglich ist die Flexibilität einer Kryptographiegrundstruktur, die eine Nationale-Flag-Karte umfasst, sehr attraktiv. Das bevorzugte Ausführungsbeispiel der Erfindung bezieht sich daher auf das Lösen von Problemen im Zusammenhang mit internationaler Kryptographie innerhalb einer Grundstruktur, die verwendet werden kann, um den Entwurf und die Entwicklung jeder nationalen Richtlinie bezüglich Kryptographie zu unterstützen.

[0042] Die Erfindung liefert eine Vielzahl von Richtlinienkonfigurationen für eine internationale Kryptographiegrundstruktur, die vier Dienstelemente aufweist, wobei jedes Dienstelement unterschiedliche Diensttypen anbietet. Die Erfindung wird in Verbindung mit der Kryptographiegrundstruktur erörtert, die derzeit das bevorzugte Ausführungsbeispiel der Erfindung ist. Es sollte klar sein, dass die Erfindung in anderen Systemen angewendet werden kann und daher nicht auf die hierin beschriebene Grundstruktur begrenzt ist, und auch nicht auf Anwendungen begrenzt ist, die Kryptographie unterstützen, sondern auch mit jeder Anwendung verwendet werden kann, die ein zweckgebundenes eingriffsicheres Richtlinienelement erfordert.

[0043] Obwohl es ein Hauptziel eines Systems, wie z. B. der internationalen Kryptographiegrundstruktur ist, Kontakt mit der Richtlinie beizubehalten, um eine von einer Regierung vorgegebene Disziplin in Kraft zu setzen, gibt es eine Vielzahl von Möglichkeiten und unterschiedlichen Konfigurationen, die verwendet werden könnten, um ein solches Ziel zu erreichen. Alle diese Konfigurationen können das Wesen einer internationalen Grundstruktur bewahren, d. h. die Kryptographiefunktion kann bei Abwesenheit einer Richtlinie nicht arbeiten. Die Grundannahme bei jeder der unterschiedlichen Konfigurationen, die hierin nachfolgend beschrieben sind, ist, dass die kryptographische Einheit dem Hostsystem keine kryptographischen Funktionen liefern kann, ohne in Kontakt mit der Richtlinie zu sein. Zu Erörterungszwecken ist der Begriff „in Kontakt mit" nicht darauf beschränkt, zu bedeuten, dass die Richtlinienkarte physikalisch an dieser Stelle vorliegt, sondern es ist das Wesen der Erfindung, dass es irgendwo eine Richtlinie gibt, die die kryptographische Einheit steuert, die Richtlinie könnte beispielsweise Millimeter von der kryptographischen Einheit angeordnet sein oder dieselbe könnte Kilometer entfernt von der kryptographischen Einheit angeordnet sein.

[0044] Somit können Richtlinienausführung, Speicherungs- und Steuerfunktionen zwischen der NFC und der kryptographischen Einheit aufgeteilt sein. Die Richtlinie kann beispielsweise eine softwarebasierte Richtliniensteuerfunktion sein, die in einer vertrauenswürdigen Umgebung verarbeitet wird, wie z. B. einem vertrauenswürdigen Betriebssystemkern. Ferner können die Grundstrukturelemente, die sich auf Vertrauen beziehen, z. B. die NFC, kryptographische Einheit und NSS entweder eine physikalische oder eine logische Verbindung haben. Außerdem kann die kryptographische Einheit eine softwarebasierte kryptographische Maschine sein, die eine Ausführungsrichtlinie aufweist, die in einer vertrauenswürdigen Umgebung gesteuert wird, wie z. B. einem vertrauenswürdigen Betriebssystemkern.

[0045] Die Richtlinie selbst hat keinen Zugriff zu anderen Daten, wie z. B. Benutzerdaten, die in der kryptographischen Einheit verarbeitet werden. Somit erlaubt die Richtlinie keine Informationen, die ihre Integrität beeinträchtigen könnten. Folglich bleibt die kryptographische Einheit, wie sie durch eine gegebene Richtlinie gesteuert wird, für alle Konfigurationen deterministisch.

[0046] Eine weitere Anforderung des Systems ist, dass die Richtlinie wissen muss, welche kryptographische Einheit dieselbe steuert, obwohl eine kryptographische Einheit nicht wissen muss, durch welche Richtlinie sie gesteuert wird. Somit steuert die Richtlinie nur eine deterministische Anzahl, d. h. eine hauptsächliche spezifische oder identifizierte, von kryptographischen Einheiten. Es ist möglich, dass

dieselben durch einen NSS aktualisiert werden.

[0047] Außerdem können entweder die kryptographische Einheit oder die Richtlinie Dienste des NSS anfordern, was wiederum die weitere Verteilung oder Delegation der Richtlinienfunktion zu einem Online-Netzwerk-Sicherheitsserver anstatt einer physikalischen Token-Karte ermöglicht. Bei diesem Ausführungsbeispiel der Erfindung liegt die Karte selbst an dem Netzwerksicherheitsserver vor und kann daher eine oder mehrere kryptographische Einheiten beinahe in Echtzeit aktivieren. Beispielsweise wird eine neue kryptographische Einheit in einem System installiert. Die neue Einheit greift für Aktivierung auf den NSS zu. Weil die Richtlinie installiert ist, wird es dem System erlaubt, die Verwendung der Kryptographie fortzusetzen. Bei diesem Beispiel ist es eine der Funktionen der Richtlinie, die Hinzufügung der neuen Einheit zu erlauben. Die Richtlinie aktiviert die Einheit durch den NSS, der wiederum Aktivierung an die Einheit sendet. Falls somit der Name des neuen Benutzers oder der Einheit in der Richtlinie ist, ermöglicht die Richtlinie Aktivierung des Benutzers/der Einheit. Dieser Aspekt der Erfindung ermöglicht es, dass das System sehr dynamisch ist und dennoch physikalische Steuerung des Systems beibehält, so dass die beabsichtigte Anwendung (bei diesem Beispiel Kryptographie) verloren ist, falls die Richtlinie von dem NSS entfernt wird. Dieses Ausführungsbeispiel der Erfindung bewahrt die physikalische Charakteristik der Richtlinie innerhalb der Grundstruktur, auch wenn die Richtlinie in einer sehr dynamischen Umgebung angewendet wird. Folglich steuert die Richtlinie den Betrieb jeder spezifischen kryptographischen Einheit.

[0048] Die folgende Erörterung bezieht sich auf die Dienstelementendpunkte und Kommunikationscharakteristika.

[0049] **Fig.** 4a ist eine schematische Darstellung, die physikalische und logische Verbindungsendpunkte der vier Grundstrukturdienstelemente einer nicht vertrauenswürdigen Umgebung darstellt; Fig. 4b ist eine schematische Darstellung, die physikalische und logische Verbindungsendpunkte der vier Grundstrukturdienstelemente in einer vertrauenswürdigen Umgebung darstellt.

[0050] Insbesondere stellt Fig. 4b die vertrauenswürdige Verarbeitungsfähigkeit dar, die sowohl den vertrauenswürdigen Kommunikationskanal als auch den Informationsgeheimhaltungsschutz unterstützt. Verallgemeinerungs- und Beziehungsmodelle. Um den Fall von Formfaktoren verallgemeinern zu können und sich hauptsächlich auf die Variabilität der Verbindungen und Interaktionen zwischen den wesentlichen Elementen, NFC, kryptographische Einheit, HS uns NSS, zu konzentrieren, sind die Figuren folgendermaßen: Physikalisch verbundene Endpunkte, die sich auf physikalische Verbindungen beziehen, sind durch durchgezogene Linien dargestellt und gestrichelte Linien stellen logische Verbindungen dar.

[0051] Die beiden Dienstelemente, die kryptographische Einheit **14** und die Richtlinie **12**, sind jeweils über einen Endpunkt verbunden, der durch eine physikalische Einrichtung dargestellt ist, der aus drei Grundkomponenten besteht: dem Richtlinienträger – der die Richtlinie selbst speichert und sicher schützt, dem Richtlinienleser R – der die Richtlinie von dem Träger extrahiert, und eine Kommunikationsverbindung, die eine brauchbare Kommunikation zwischen dem Leser und dem Peer-Empfänger in dem Hostsystem beibehält.

[0052] Der Sender und der Empfänger haben ein kompatibles Kommunikationssystem oder dieselben sind mit einem Netzübergang verbunden, dessen Funktion es ist, heterogene Kommunikationsstandards umzuwandeln. Die letztere Kommunikationsverbindung kann auf ein vermaschtes Netzwerk verschiedener Kommunikationsstandards erweitert werden. Jeder Endpunkt der Kommunikationsverbindung ist mit dem Richtlinienleser R auf der einen Seite und dem Peer-Empfänger auf der anderen Seite kompatibel.

[0053] Ein Übergang von vertrauenswürdigen physikalischen Komponenten zu der vertrauenswürdigen Ausführung logischer Komponenten. Fig. 5a–Fig. 5f sind schematische Blockdiagramme, die die n-äre Beziehungen zwischen den Grundstrukturelementen durch Verbindungsendpunkte darstellen, die zwischen einer Richtlinie und einer kryptographischen Einheit hergestellt sind. Drei Beispiele können gegeben werden, um die Flexibilität der Architektur darzustellen, wenn mit verschiedenen physikalischen Elementen gearbeitet wird.

[0054] Beispiel 1: A-1-zu-1-Fall. Ein Richtlinienträger ist eine Kontakt-/kontaktlose Smartcard, der Richtlinienleser R ist der Kontakt-/kontaktlose Leser, der die Informationen über eine RS232-Leitung zu einer kryptographischen Einheit überträgt, die durch eine interne Busplatine mit einem Chip dargestellt ist. Ein Beispiel dieses Falls ist durch eine PCI-Platine mit einem Plug-in-Chip dargestellt. Die Kommunikation mit der NFC wird durch eine Eingabe/Ausgabe-Steuerung für eine RS232-Verbindung hergestellt, die auf einem entfernten System angeordnet ist.

[0055] Beispiel 2: Ein N-zu-1-Fall. Ein Richtlinienträger ist eine Kontaktsmartcard, die Richtlinienleser Rs sind die Kontaktleser, die an eine Platine angebunden sind, die eine N-zu-1-Beziehung ermöglichen. Ein Beispiel einer Darstellung ist die gleiche PCI-Platine mit 8 angebundenen Lesern.

[0056] Beispiel 3: Ein Kaskadenfall. Der Richtlinienträger ist eine Kontaktsmartcard, die Richtlinienleser Rs sind die Kontaktleser, die an eine kryptographische Einheit angebunden sind, die ferner die Richtliniensteuerungen an die P-Endnutzerkryptographieeinheiten delegiert. Mit dem Telekommunikationsbeispiel einer GSM-Infrastruktur, d. h. einem globalen System für Mobilkommunikation, stellt das AUC – Authentifizierungszentrum – die Zwischen-P-CUs dar und die GSM-Telefone sind die M-Endnutzer. Die Telekommunikationsinfrastruktur liefert die Einrichtung für die Endpunktverbindungen für die NFCs und die kryptographischen Einheiten.

[0057] NFC-zu-NSS-Kommunikation. Bevor die Erörterung zwischen der NFC und der kryptographischen Einheit begonnen wird, ist es wichtig, das vertrauenswürdige Richtliniensteuersystem des NSS als eine Anwendung der vorhergehenden Fälle von NFC zu kryptographischer Einheit zu betrachten.

[0058] Zwei Hauptkategorien der Interaktionen werden zwischen der NFC und dem NSS identifiziert:

- Die erste Kategorie umfasst alle Attribute, die sich auf die Erneuerung von Verwendungen für einen bereits verwendeten Algorithmus, ein Schlüsselverwaltungsschema oder Beschränkungsdaten beziehen. Weitere Aktualisierungen des Verschlüsselungsmaterials, der geheimen Daten und der Zeitwerte sind ebenfalls Teil dieser Kategorie. Die Installation neuer Richtlinien, der Austausch und die Veralterung bestehender Richtlinien sind der letzte Punkt innerhalb dieser Kategorie.
- Die zweite Kategorie umfasst die abnormalen Verhaltensweisen der kryptographischen Einheit, die Erfassung aktiver Attacken oder den Austausch vertrauenswürdiger Komponenten.

[0059] Beide Beziehungskategorien basieren auf einer eingebauten Interaktikonsrichtlinie zwischen der NFC und dem NSS. Beide Interaktionskategorien können in dem Beziehungsmodell ausgedrückt werden, wie es in Fig. 6a–Fig. 6f dargestellt ist, die schematische Blockdiagramme sind, die die n-ären Beziehungen zwischen den Grundelementen durch Verbindungsendpunkte darstellen, die zwischen einer Richtlinie und einem NSS hergestellt sind.

[0060] Ein bestimmter Fall ist die Kaskade. Die Kaskade stellt eine typische Delegationsstruktur dar, ähnlich einer Zertifizierungshierarchie innerhalb eines Netzwerks von vertrauenswürdigen dritten Parteien (TTP). Ein Beispiel dieser Struktur ist ein vermaschtes Netzwerk von TTPs in Europa, zwischen Großbritannien, Frankreich und Deutschland, die auf der Basis nationaler TTP-Darstellungen ein gemeinsames Schlüsselwiedergewinnungsschema implementieren.

[0061] Logische Komponenten. Eine weitere potentielle Darstellung des Richtlinienträgers kann eine durch einen vertrauenswürdigen Prozessor gesteuerte Software umfassen, die sich in einer Host-CPU befindet.

[0062] Die Kommunikationsmechanismen sind die bestehenden Zwischenprozesskommunikationssysteme und der Kommunikationsvermittler sind die Hüllkurven.

[0063] Vertrauenswürdige gegen nicht vertrauenswürdige Verarbeitungsumgebung. Durch den Aufbau ist die implizite Interaktionsrichtlinie in die vertrauenswürdigen Dienstelemente eingebaut. Daher verlässt sich jedes Dienstelement, die kryptographische Einheit, die NFC, der Host oder der NSS auf eine vertrauenswürdige Ausführungsfähigkeit, um den Kommunikationskanal einzurichten. Darüber hinaus muss der Verursacher auch dem Empfänger vertrauen, dass derselbe die geheimen Informationen – Berührungspunktdaten – aufrechterhält, sobald die Informationen an den Empfänger geliefert werden.

[0064] Fig. 7a–Fig. 7c liefern ein schematisches Blockdiagramm eines zweckgebundenen Richtlinienelements gemäß drei alternativen Anordnungen eines ersten bevorzugten Ausführungsbeispiels der Erfindung.

[0065] In Fig. 7a ist die Richtlinie **12** mit der kryptographischen Einheit **14** durch einen eingebauten Smartcardleser **40** verbunden, wobei der Smartcardleser nur der Funktion des Verbindens der Richtlinie mit der kryptographischen Einheit zugewiesen ist. Die kryptographische Einheit wird dann mit dem Hostsystem **16** verbunden. Wo die kryptographische Einheit beispielsweise eine Schaltungskarte ist, wird die Schaltungskarte in einen Schlitz auf der Hostsystemhauptplatine eingesteckt (siehe Fig. 7b). Der Scanner selbst kann jede gut bekannte Scanvorrichtung sein, die in der Lage ist, eine Smartcard zu lesen.

[0066] Bei dem Beispiel von Fig. 7b, wo die kryptographische Einheit **14** auf einer Schaltungskarte **44** befestigt ist, umfasst die kryptographische Einheit eine eingriffsichere Anschlussfläche und Behälter, die auf der Schaltungskarte befestigt sind und somit einen zusätzlichen Eingriffsschutz liefern. Die Schaltungskarte ist mit der Hostsystemhauptplatine **46** durch einen Schlitz **45** verbunden. Leiterbahnen **42** auf der Schaltungsplatine führen zu einem Schubfach an der Rückseite des Hostsystems **16**, d. h. des Computers, das dazu dient, die Richtlinie **12** in einem festverdrahteten Aufnahmeelement oder anderem Tor aufzunehmen, wie z. B. dem Smartcardleser **40**.

[0067] Bei dem Beispiel von Fig. 7c ist die kryptographische Einheit **14** direkt auf der Hauptplatine **46** befestigt und die Richtlinie **12** ist mit der kryptographi-

schen Einheit verbunden, beispielsweise über ein Aufnahmeelement in der kryptographischen Einheit oder in der Hauptplatine selbst.

[0068] Bei allen drei Beispielen oben kann ein Smartcardleser verwendet werden, um die Richtlinie mit der kryptographischen Einheit zu verbinden, wobei der Smartcardleser sowohl zweckgebunden ist zum Lesen nur dieser Richtlinie und wobei derselbe eingebaut ist in die kryptographische Einheit oder derselben unmittelbar zugeordnet ist.

[0069] Fig. 8 ist ein schematisches Blockdiagramm eines weiteren zweckgebundenen Richtlinienelements gemäß einem zweiten bevorzugten Ausführungsbeispiel der Erfindung. Bei diesem Ausführungsbeispiel der Erfindung ist die kryptographische Einheit **14** auf einer Schaltungskarte **44** befestigt, und die Schaltungskarte ist über einen Hauptplatinenschlitz **45** mit der Hostsystemhauptplatine **46** verbunden. Die kryptographische Einheit ist durch verschiedene Leitungen oder Leiterbahnen **42** mit einem Verbinder **53** auf der Schaltungskarte verbunden. Bei einem Ausführungsbeispiel der Erfindung liefert der Verbinder ein Standard-RS-232-Tor, so dass die Schaltungskarte ein serielles Tor umfasst.

[0070] Ein getrennter zweckgebundener Smartcardleser **40** weist einen Verbinder **54** auf, der es einem Kabel **50** ermöglicht, den Smartcardleser mit der Schaltungskarte an dem Schaltungskartenverbinder **52** zu verbinden. Die Richtlinie **12** wird durch den Smartcardleser **40** gelesen. Somit ist bei diesem Ausführungsbeispiel der Erfindung der Smartcardleser zweckgebunden und lokal für den Host, ist aber entfernt von der kryptographischen Einheit angeordnet, d. h. nicht in die kryptographische Einheit eingebaut.

[0071] Fig. 9 ist ein schematisches Blockdiagramm eines gemeinschaftlich verwendeten Richtlinienelements gemäß einem dritten bevorzugten Ausführungsbeispiel der Erfindung. Bei diesem Ausführungsbeispiel der Erfindung ist die kryptographische Einheit **14** auf einer Schaltungskarte **44** befestigt und die Schaltungskarte ist über einen Hauptplatinenschlitz **45** mit der Hostsystemhauptplatine **46** verbunden. Die kryptographische Einheit ist durch verschiedene Leiterbahnen oder Leitungen **42** mit einem Verbinder **52** auf der Schaltungskarte verbunden. Bei einem Ausführungsbeispiel der Erfindung liefert der Verbinder ein Standard-RS-232-Tor, so dass die Schaltungskarte ein serielles Tor aufweist.

[0072] Ein getrennter gemeinschaftlich verwendeter Smartcardleser **40** weist einen Verbinder **54** auf, der es einem Kabel **50** ermöglicht, den Smartcardleser mit der Schaltungskarte an dem Schaltungskartenverbinder **52** zu verbinden. Die Richtlinie **12** wird durch den Smartcardleser **40** gelesen, wie bei dem Ausführungsbeispiel der Erfindung, das in Fig. 8 oben gezeigt ist.

[0073] Es ist jedoch sowohl teuer als auch ineffizient, einen Smartcardleser zu schaffen, dessen einzige Funktion es ist, die Richtlinie zu halten. Bei diesem Ausführungsbeispiel der Erfindung kann der Smartcardleser verwendet werden, um andere Smartcards **60**, **62**, **64** zu lesen, um andere Funktionen **66**, **68** zu verwenden, die auf der Schaltungskarte **44** oder Hauptplatine **46** vorgesehen sein können oder nicht. Diese Konfiguration wird als gemeinschaftlich verwendet bezeichnet, weil der Smartcardleser mit einer Richtlinie und beispielsweise einer ID-Karte gemeinschaftlich verwendet wird, während bei den vorher erörterten Ausführungsbeispielen der Erfindung der Smartcardleser zweckgebunden war zum Durchführen von nur einer Richtlinienlesefunktion.

[0074] Bei einer Form dieses Ausführungsbeispiels wird die Funktionalität der Richtlinie **12** in eine Smartcard **72** eingesetzt, zusammen mit einer ID-Kartenfunktion **70**, so dass es in einer Smartcard eine Funktionalität für sowohl eine ID als auch eine Richtlinie gibt. Dieses Ausführungsbeispiel der Erfindung ist sinnvoll für Anwendungen wie z. B. einen Ausweis oder ein Visum, die sowohl Staatsangehörigkeitsberechtigungsnachweise als auch Autorisierung für die Verwendung von Kryptographie umfassen würden. Somit informiert die Smartcard nicht nur eine Behörde oder ein System über die Identität des Benutzers, sondern aktiviert auch Kryptographie gemäß der Regierungsrichtlinie.

[0075] Bei dieser Verwendung aktiviert diese gemeinschaftlich verwendete Konfiguration die kryptographische Funktion und umfasst weitere Funktionen, wie z. B. ID, die auch bestimmte Privilegien umfassen können. Die gemeinschaftlich verwendete Konfiguration lässt das System die Identität des Benutzers wissen und aktiviert dadurch solche Privilegien, setzt die Sicherheit in Kraft und erzeugt einen Prüfweg der Verwendung des Systems, zusätzlich zum Aktivieren der kryptographischen Funktion.

[0076] In der Sicherheitsindustrie gibt es einen Unterschied zwischen Rechten und Fähigkeiten. Dieses Ausführungsbeispiel der Erfindung liefert eine Smartcard, die einem Benutzer sowohl Rechte zum Verwenden von Kryptographie liefert als auch die Kryptographie mit bestimmten Fähigkeiten aktiviert. Somit liefert eine gemeinschaftlich verwendete Smartcardkonfiguration sowohl Recht als auch Fähigkeit auf individueller Basis.

[0077] Weil der Smartcardleser gemeinschaftlich verwendet wird, können getrennte Smartcards für unterschiedliche Einzelpersonen und unterschiedliche Funktionen verwendet werden. Beispielsweise kann

eine Richtlinie durch den Smartcardleser gelesen werden, wobei die Richtlinie eine von mehreren Funktionen auf einer Smartcard sein kann, so dass der Träger der Karte Rechte empfängt, Kryptographie zu verwenden, sowie weitere Rechte/Privilegien. Andere Nutzer des Systems können eine Smartcard haben, die keine Richtlinie hat. Für solche Einzelpersonen existiert keine Kryptographie in dem System, obwohl diese Einzelpersonen bestimmte andere Rechte und/oder Fähigkeiten haben können. In beiden Fällen kann eine ID-Funktion, die der Smartcard zugeordnet ist, vorgesehen sein, die dazu dient, Zugriff zu dem System zu steuern, während ein Prüfweg der Systemverwendung beibehalten wird.

[0078] Somit wird bei diesem Ausführungsbeispiel der Erfindung der Smartcardleser für mehrere Zwecke verwendet, d. h. er wird gemeinschaftlich verwendet zwischen der Richtlinie und anderen Funktionen und ist lokal in dem Host, ist aber entfernt von der kryptographischen Einheit angeordnet, d. h. ist nicht in die kryptographische Einheit eingebaut.

[0079] Fig. 10 ist ein schematisches Blockdiagramm noch eines weiteren zweckgebundenen Richtlinienelements gemäß einem vierten bevorzugten Ausführungsbeispiel der Erfindung. Bei diesem Ausführungsbeispiel der Erfindung ist der Host über ein Netzwerk **70**, **71**, **72** mit einem anderen Host verbunden, der eine der oben beschriebenen Kombinationen der kryptographischen Einheit **14** und Richtlinie **12** aufweist. Die entfernte kryptographische Einheit **84** wird von der Richtlinie **12** über das Netzwerk aktiviert. Die entfernte kryptographische Einheit kann ansonsten wie oben konfiguriert sein, z. B. auf einer Schaltungskarte **74** befestigt sein, die über einen Kartenschlitz **75** auf der Hauptplatine mit einer Hauptplatine **76** verbunden ist.

[0080] Bei einer Form dieses Ausführungsbeispiels der Erfindung steuert die Richtlinie eine kleine Anzahl von kryptographischen Einheiten durch das Netzwerk. Die Anzahl von kryptographischen Einheiten, die die Richtlinie über das Netzwerk verwaltet, ist durch die Fähigkeit der Bandbreite der Richtlinie beim Verarbeiten von Leistung begrenzt. Um diese Begrenzung der Richtlinie zu adressieren, liefert eine weitere Form dieses Ausführungsbeispiels der Erfindung eine Aktivierungsfunktionalität an einer ersten kryptographischen Einheit **14**, die von der Richtlinie zu der kryptographischen Einheit **14** übertragen wird. Die kryptographische Einheit wiederum aktiviert alle anderen kryptographischen Einheiten in dem System. Falls die Richtlinie entfernt wird, verliert die primäre kryptographische Einheit ihre Funktion und mit derselben verlieren alle anderen kryptographischen Einheiten ihre Funktion. Somit wird eine leistungsfähigere kryptographische Einheit befähigt, andere kryptographische Einheiten zu aktivieren, alle gemäß und unter der Steuerung einer Richtlinie, wobei die Richtlinie die primäre kryptographische Einheit bezüglich dessen anweist, welche anderen Einheiten aktiviert werden dürfen, wer diese Einheiten verwenden kann und welche Rechte/Fähigkeiten für solche Benutzer gelten.

[0081] Obwohl die Erfindung hierin mit Bezugnahme auf das bevorzugte Ausführungsbeispiel beschrieben ist, erkennt ein Durchschnittsfachmann auf diesem Gebiet ohne weiteres, dass andere Anwendungen für diejenigen eingesetzt werden können, die hierin aufgeführt sind, ohne von dem Schutzbereich der vorliegenden Erfindung abzuweichen. Folglich soll die Erfindung nur durch die nachfolgend angehängten Ansprüche begrenzt sein.

Patentansprüche

1. Kryptographiegrundstruktur zum Liefern einer einheitlichen Verschlüsselung, die vereinbar und in Übereinstimmung mit verschiedenen nationalen, regionalen, Industrie- oder Behördenkryptographierichtlinien arbeitet, die folgende Merkmale umfasst:
eine Richtlinie (**112**), die angepasst ist, um ein Kryptographieschema aufzunehmen, das von einer bestimmten nationalen, regionalen, Industrie- oder Behördenkryptographierichtlinie der Domain, in der die Grundstruktur verwendet wird, gefordert wird, wobei die Richtlinie angepasst ist, um sicherzustellen, dass eine allgemeine Kryptographiemaschine und die Verwendung derselben mit nationalen, regionalen, Industrie-, oder Behördenkryptographierichtlinien in einer Domain, in der die Grundstruktur verwendet wird, übereinstimmen;
eine Kryptographieeinheit (**14**), die eine Kryptographiemaschine umfasst, wobei die Kryptographieeinheit angepasst ist, um das Kryptographieschema zu implementieren, wobei die Richtlinie mit der Kryptographieeinheit verbunden ist, sodass Kryptographiefunktionen bei Abwesenheit dieser Richtlinie nicht ausgeführt werden können, wobei die Kryptographieeinheit eine allgemeine Kryptographiemaschine implementiert;
ein Hostsystem (**16**), das angepasst ist, um eine Informationstechnologieanwendung zu implementieren, wobei das Hostsystem für Kommunikation mit der Kryptographieeinheit angeordnet ist, und angepasst ist, um das Kryptographieschema zu implementieren, falls und nur falls das Hostsystem in Kombination mit einer Kryptographieeinheit und einer gültigen Richtlinie verwendet wird; und
zumindest einen Leser (R) zum Verbinden einer Richtlinienkarte, die die Richtlinie enthält, mit der Kryptographieeinheit;
dadurch gekennzeichnet, dass die Richtlinie (**12**) den Betrieb einer Primärkryptographieeinheit steuert, die wiederum den Betrieb von einer oder mehreren Kryptographieeinheiten aktiviert und steuert, wobei die Primärkryptographieeinheit und die eine oder mehreren anderen Kryptographieeinheiten ihre

Funktion verlieren, falls die Richtlinienkarte von dem Leser entfernt wird.

2. Die Grundstruktur gemäß Anspruch 1, bei der der Leser (R) ein gemeinschaftlich verwendeter Leser ist.

3. Die Grundstruktur gemäß Anspruch 1, bei der der Leser (R) in die Kryptographieeinheit eingebaut ist.

4. Die Grundstruktur gemäß Anspruch 1, bei der sich der Leser (R) lokal in der Kryptographieeinheit befindet.

5. Die Grundstruktur gemäß Anspruch 1, bei der der Leser entfernt von der Kryptographieeinheit ist.

6. Die Grundstruktur gemäß Anspruch 1, bei der der Leser (R) ein zweckgebundener Leser ist.

7. Die Grundstruktur gemäß Anspruch 1 oder 2, bei der die Kryptographieeinheit (**14**) angepasst ist, um die Richtlinie darin zu empfangen und zu sichern.

8. Die Grundstruktur gemäß einem der Ansprüche 1 bis 7, bei der die Richtlinie (**12**) angepasst ist, um selektiv zumindest einen zusätzlichen Kryptographiestandard in Kombination mit der Kryptographieeinheit zu implementieren.

9. Die Grundstruktur gemäß Anspruch 8, bei der der ausgewählte Kryptographiestandard einen aus einem ausgewählten Kryptographiealgorithmus, einer ausgewählten Kryptographieebene, einer nationalen Richtlinie, Informationspersonalisierung, System- und Netzwerkzugriffsmessung und erneuerbarer Kryptographie umfassen kann.

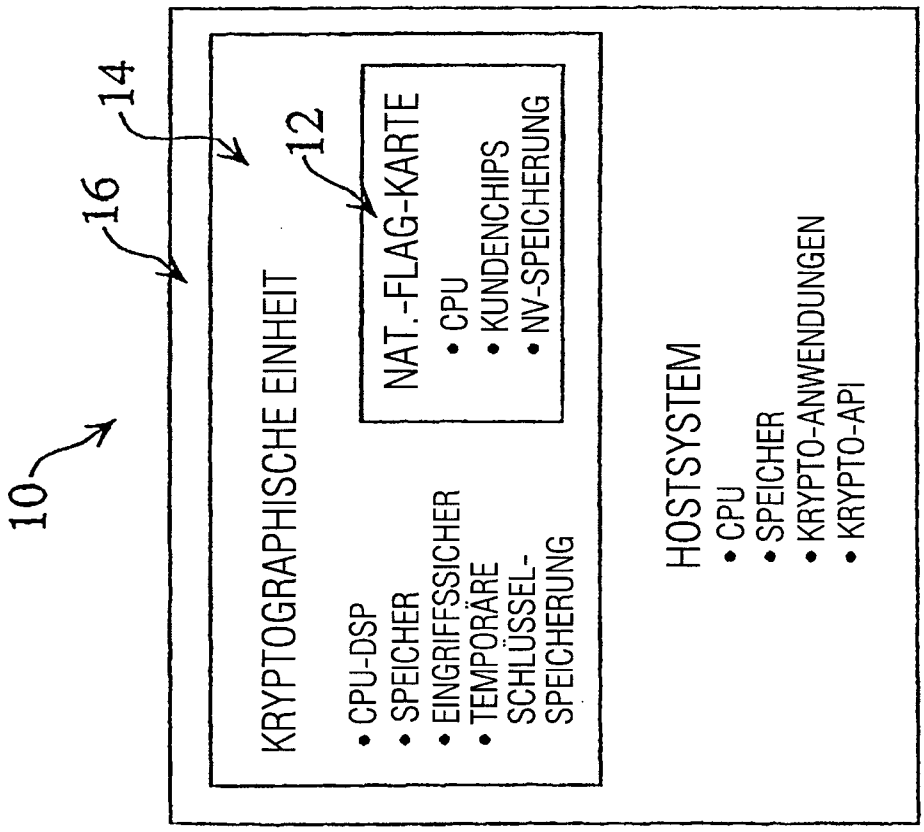
10. Die Grundstruktur gemäß Anspruch 8, wobei der zumindest eine andere Standard einen aus Einrichten einer Identität, Einrichten von Privilegien, Einrichten von Rechten, Einrichten von Fähigkeiten, In-Kraft-Setzen von Sicherheit und Erzeugen eines Prüfpfads umfasst.

11. Die Grundstruktur gemäß Anspruch 1, bei die Richtlinie (**12**) eine eingriffssichere Smartcard ist.

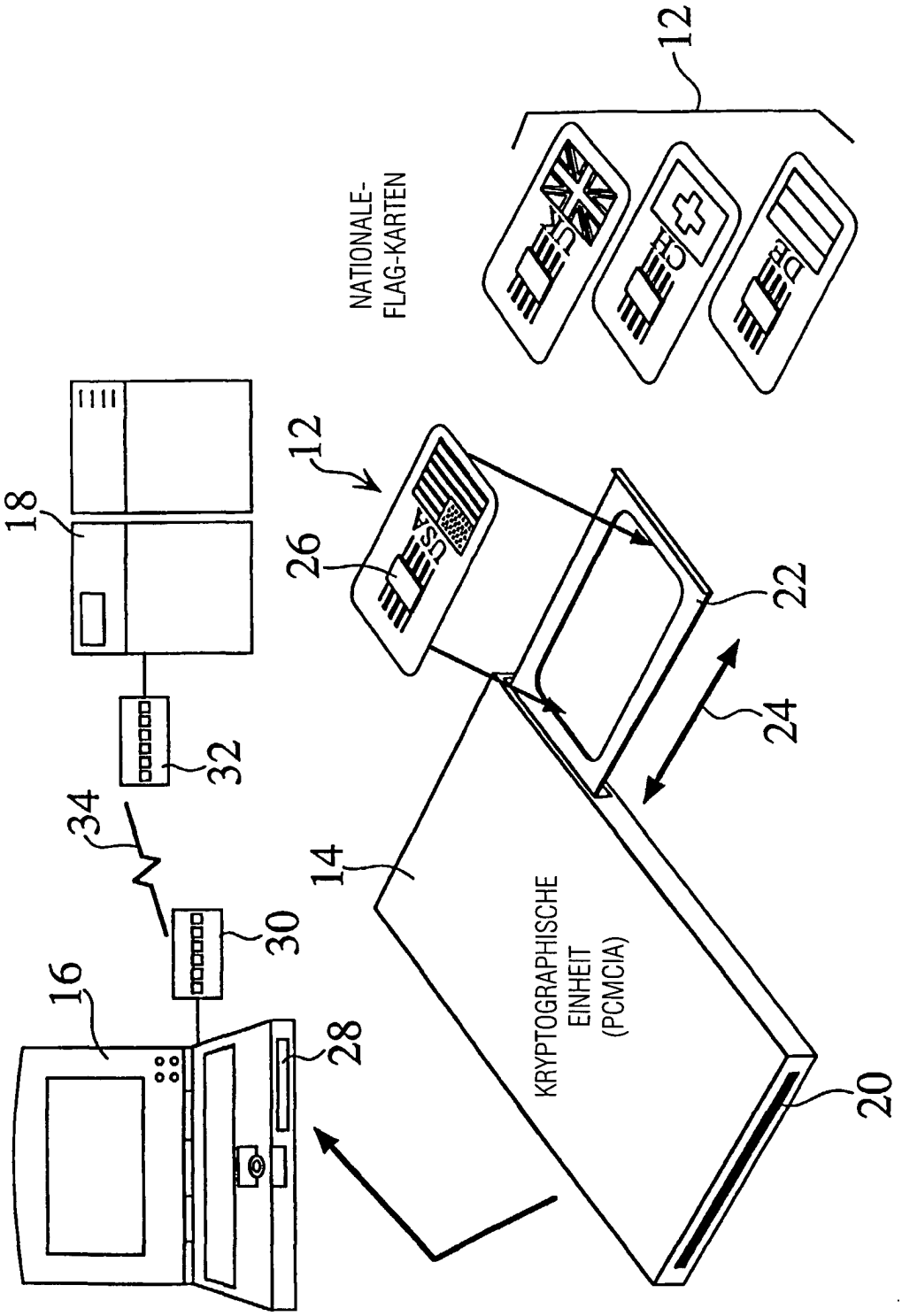
12. Die Grundstruktur gemäß einem der Ansprüche 1 bis 11, bei der die Richtlinie (**12**) den Betrieb von mehr als einer Kryptographieeinheit steuert.

Es folgen 10 Blatt Zeichnungen

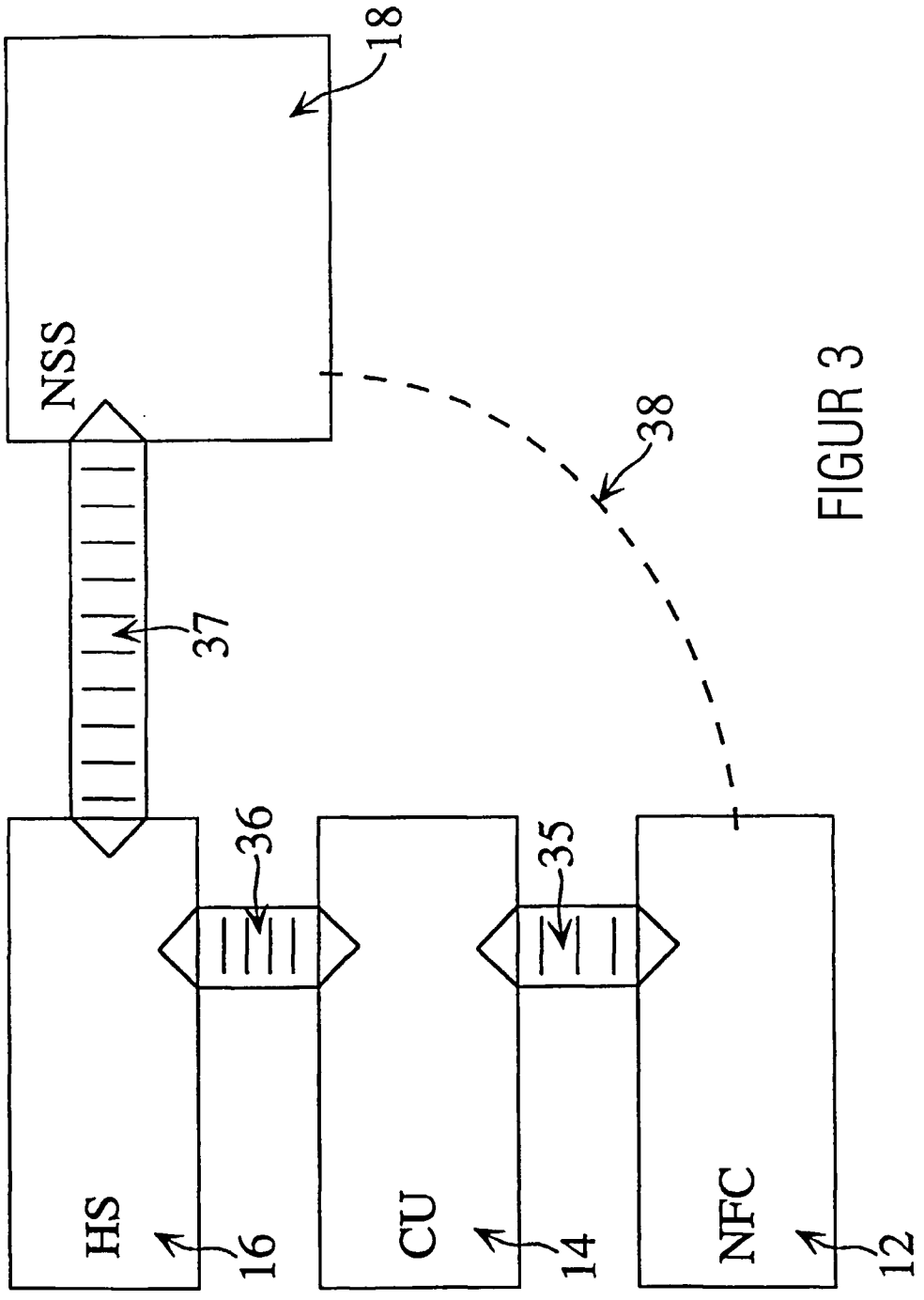
Anhängende Zeichnungen



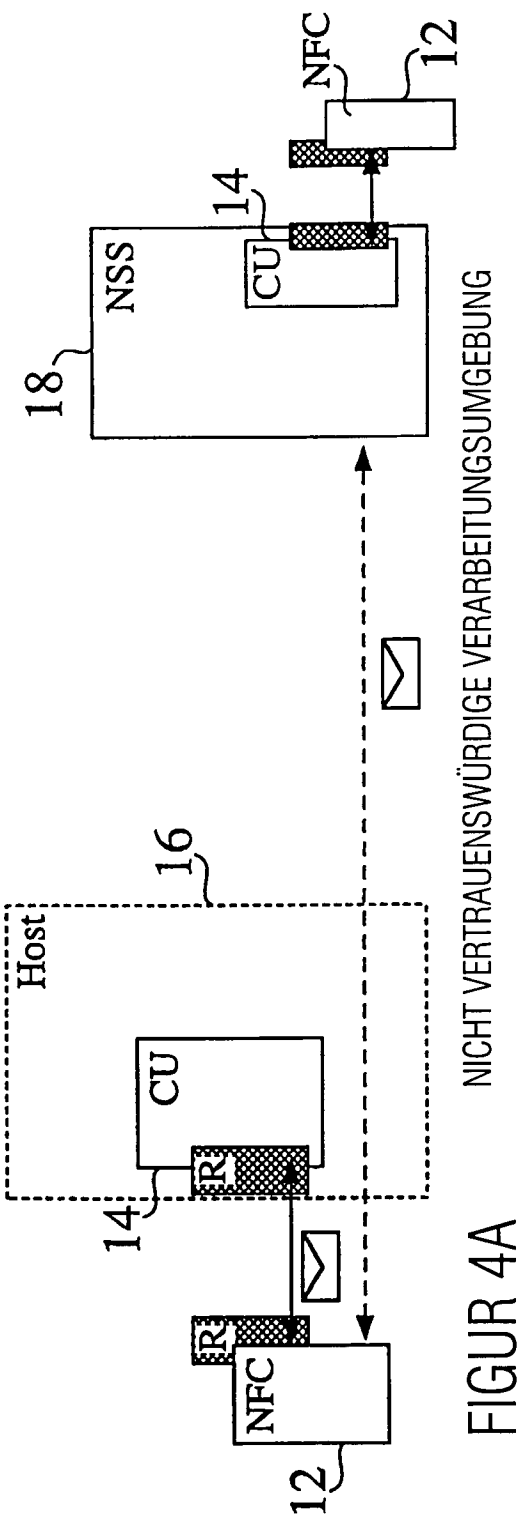
FIGUR 1
(STAND DER TECHNIK)


12
NATIONALE-
FLAG-KARTEN
18
12
26
22
24
32
34
14
KRYPTOGRAPHISCHE
EINHEIT
(PCMCIA)
30
16
28
20

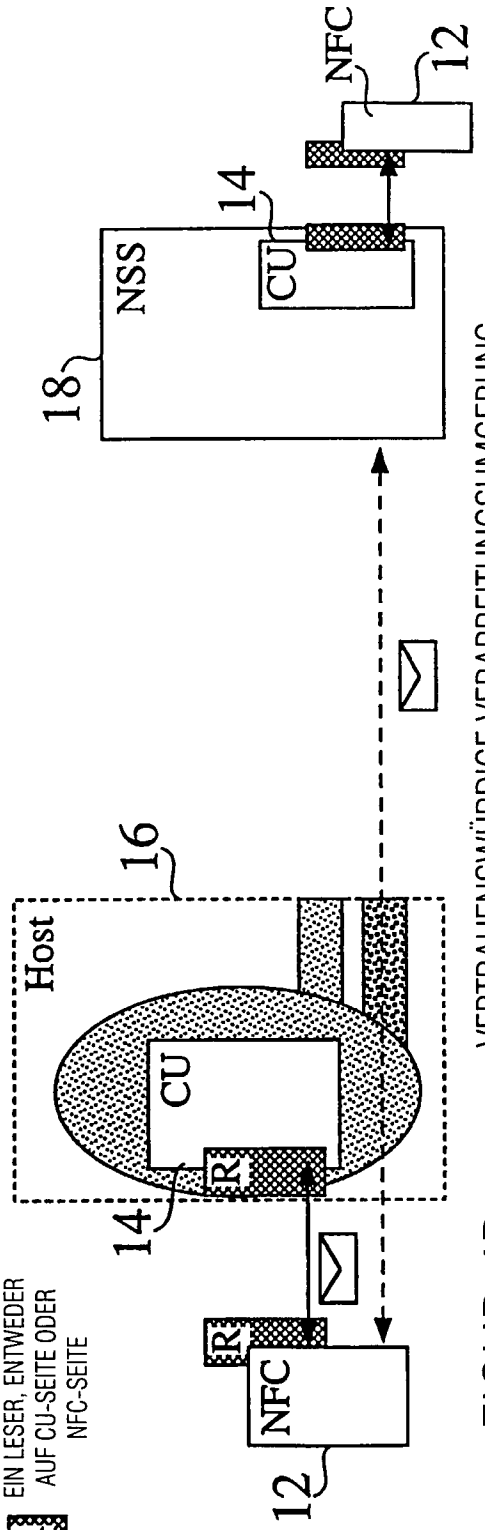
FIGUR 2



FIGUR 3

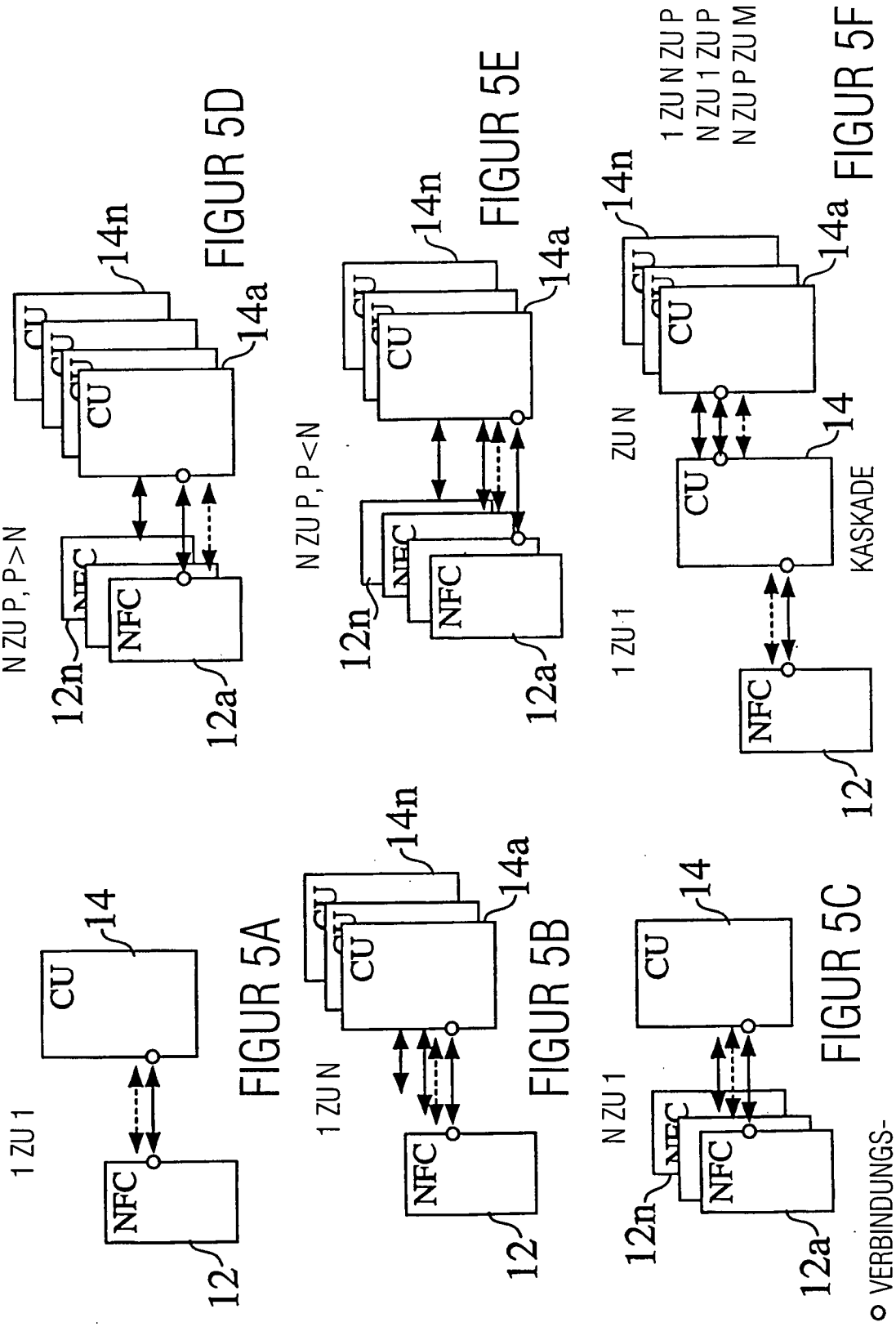


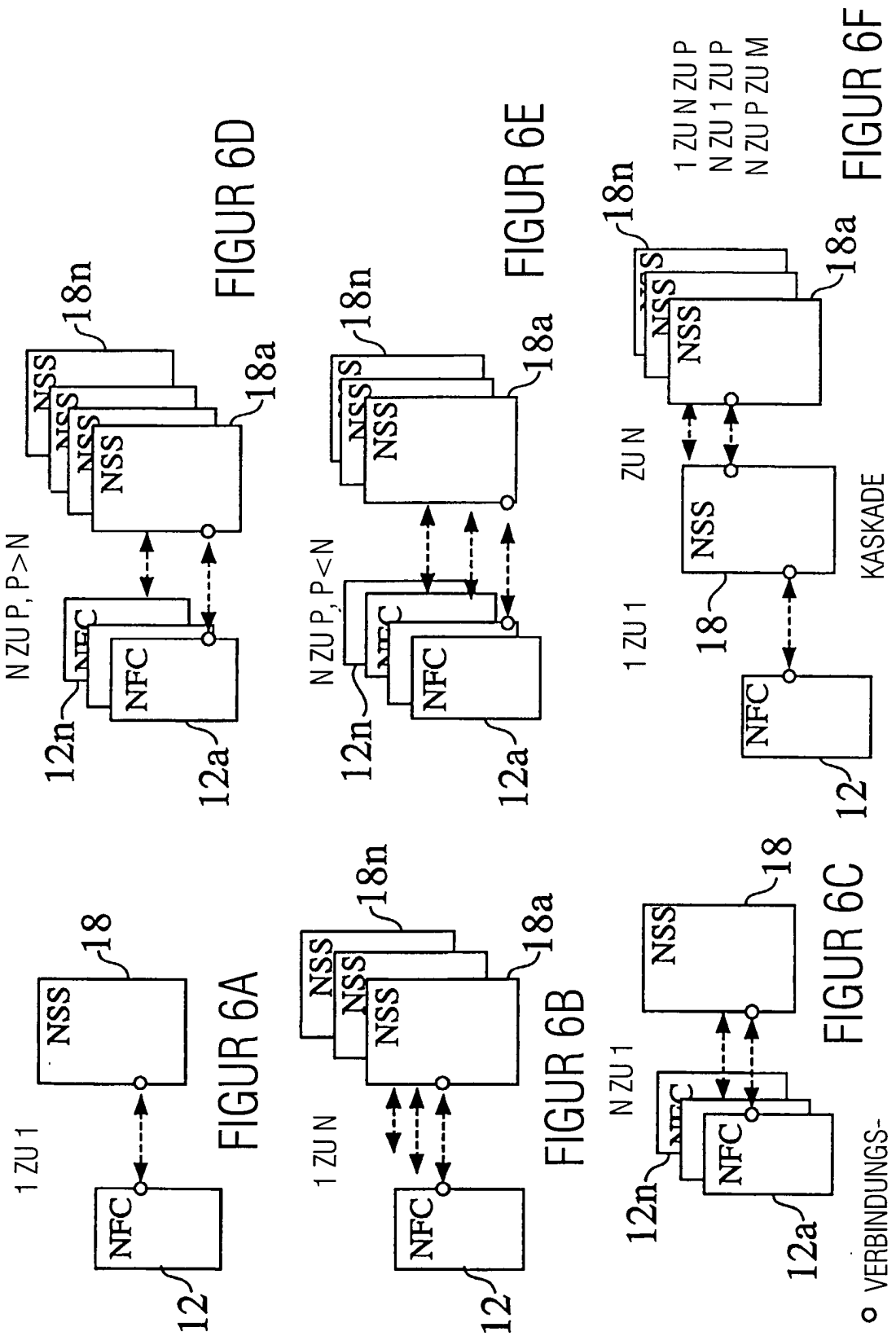
FIGUR 4A

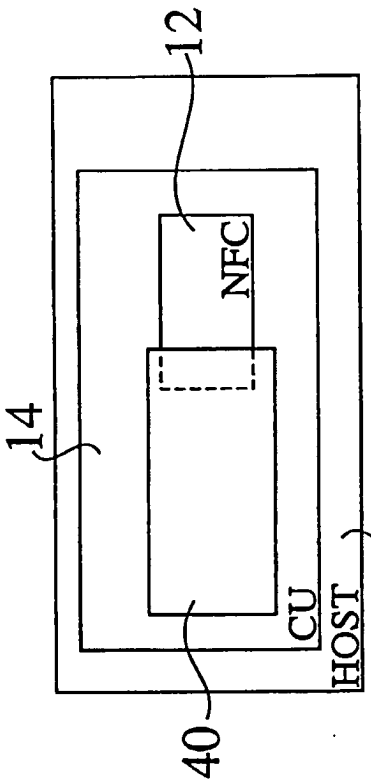


FIGUR 4B

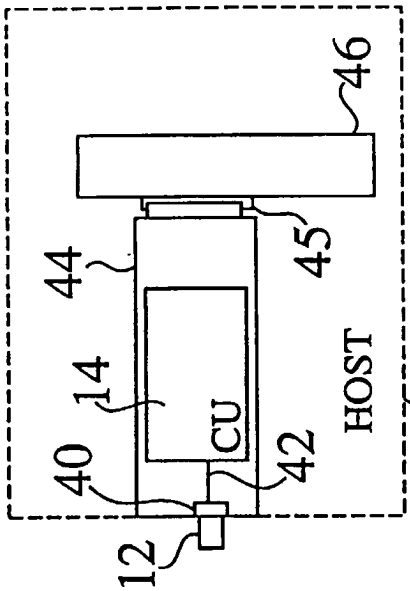
R EIN LESER, ENTWEDER AUF CU-SEITE ODER NFC-SEITE


1 ZU 1
CU
14
NFC
12
FIGUR 5A
1 ZU N
14n
14a
CU
NFC
12
FIGUR 5B
N ZU 1
14
CU
NFC
12n
12a
FIGUR 5C
N ZU P, P>N
14n
14a
CU
NFC
12n
12a
FIGUR 5D
N ZU P, P<N
14n
14a
CU
NFC
12n
12a
FIGUR 5E
1 ZU N ZU P
N ZU 1 ZU P
N ZU P ZU M
ZU N
1 ZU 1
14n
14a
14
KASKADE
NFC
12
FIGUR 5F
o VERBINDUNGS-ENDPUNKT

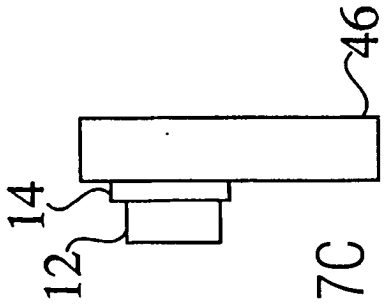

1 ZU 1
NSS
18
NFC
12
FIGUR 6A
1 ZU N
NSS
18n
18a
NFC
12
FIGUR 6B
N ZU 1
NSS
18
NFC
12a
12n
FIGUR 6C
N ZU P, P>N
NSS
18n
18a
NFC
12a
12n
FIGUR 6D
N ZU P, P<N
NSS
18n
18a
NFC
12a
12n
FIGUR 6E
1 ZU N
1 ZU N ZU P
N ZU 1 ZU P
N ZU P ZU M
NSS
18n
18a
18
1 ZU 1
KASKADE
NFC
12
FIGUR 6F
VERBINDUNGS-
ENDPUNKT



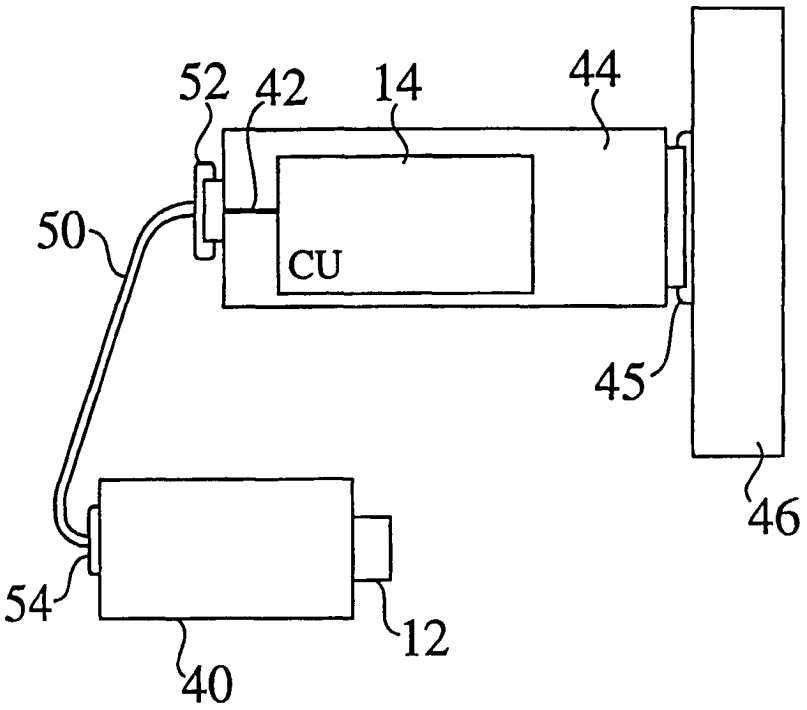
FIGUR 7A



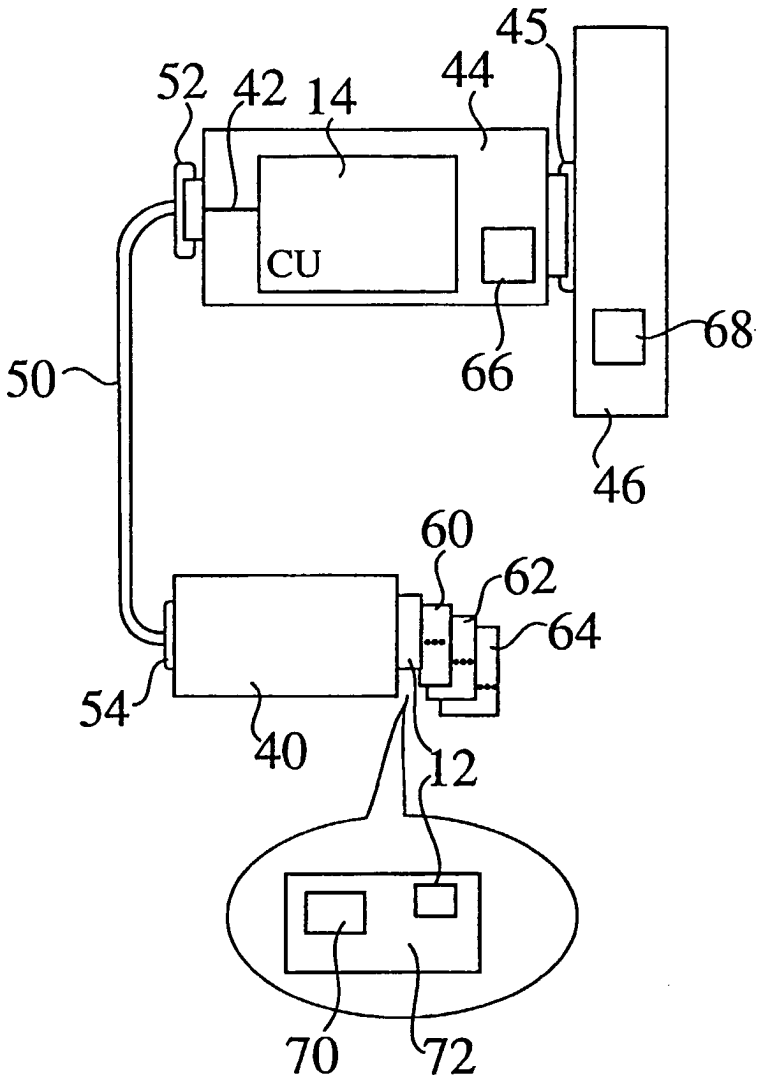
FIGUR 7B



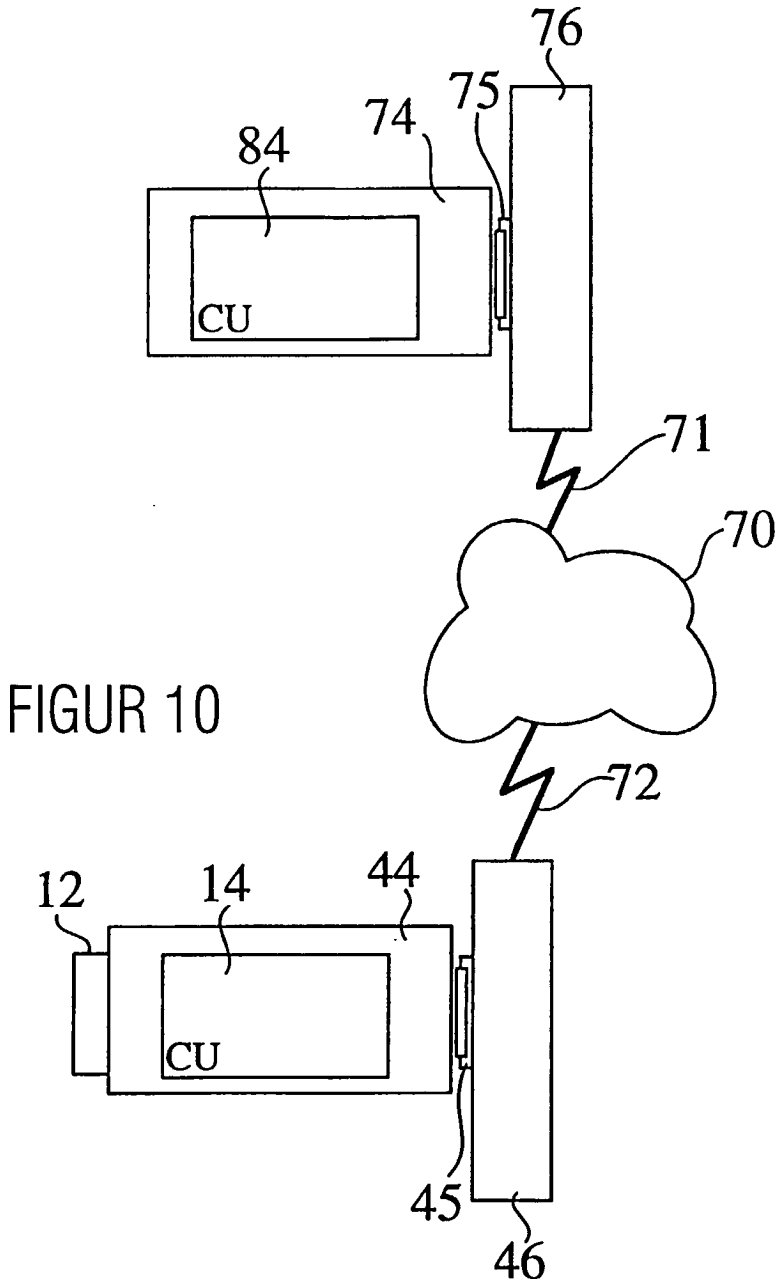
FIGUR 7C



FIGUR 8



FIGUR 9



FIGUR 10