(19) SCHWEIZERISCHE EIDGENOSSENSCHAFT
EIDGENÖSSISCHES INSTITUT FÜR GEISTIGES EIGENTUM

(11) CH 709 936 A2

(51) Int. Cl.: H04L 9/00 (2006.01)
G06F 21/60 (2013.01)

Patentanmeldung für die Schweiz und Liechtenstein
Schweizerisch-liechtensteinischer Patentschutzvertrag vom 22. Dezember 1978

(12) PATENTANMELDUNG

(21) Anmeldenummer: 01092/15

(22) Anmeldedatum: 28.07.2015

(43) Anmeldung veröffentlicht: 29.01.2016

(30) Priorität:
28.07.2014 US 62/029,678
27.02.2015 US 62/121,757
06.05.2015 US 14/705,629

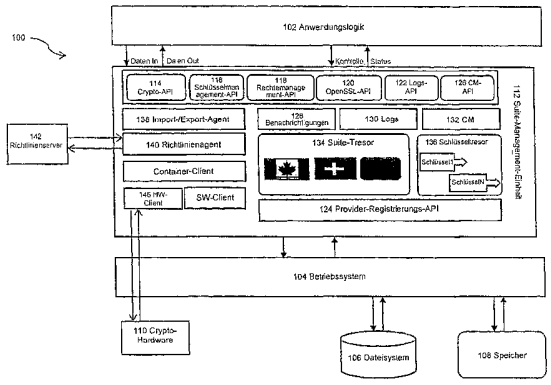
(71) Anmelder:
InfoSec Global Inc., 2225 Sheppard Avenue West, Suite 1015
M2J 5C2 Toronto, Ontario (CA)

(72) Erfinder:
Adrian Antipa, L6POE3 Brampton, Ontario (CA)
Dominic Chorafakis, L6POE3 Brampton, Ontario (CA)
Brian Neill, L6POE3 Brampton, Ontario (CA)

(74) Vertreter:
Braunpat Braun Eder AG, Reussstrasse 22
4054 Basel (CH)

(54) System und Verfahren für das kryptographische Suite-Management.

(57) Die Erfindung betrifft Systeme und Verfahren für das kryptographische Suite-Management. Ein System für das kryptographische Suite-Management weist eine kryptographische Suite-Management-Einheit (112) auf, die eine Reihe von APIs umfasst, die es verschiedenen Anwendungen ermöglichen, kryptographische Funktionen abzurufen. Das System ermöglicht: den Zugang mehrerer Anwendungen zu geteilten kryptographischen Ressourcen an einer Schnittstelle; das Teilen und Lizenzieren kryptographischer Ressourcen zwischen Geräten durch Anwendungen in mehreren Geräten; das Verschlüsseln, Entschlüsseln und Teilen von Daten zwischen Geräten mit verschiedenen kryptographischen Implementierungen; die Definition, Verbreitung und Umsetzung von Richtlinien, welche die Nutzungsbedingungen für kryptographische Implementierungen, Systeme und Verfahren bestimmen, um geteilte und dynamisch geladene kryptographische Provider zu sichern und zu schützen; die Verwendung mehrerer kryptographischer Ressourcen durch eine Anwendung und das Verwalten kryptographischer Provider-Pakete und zugehöriger Richtlinien über eine oder viele Instanzen von kryptographischen Suite-Management-Einheiten.



Beschreibung

TECHNISCHER BEREICH

[0001] Das Folgende betrifft im Allgemeinen Datenkommunikationen und insbesondere Systeme und Verfahren zur Sicherung von Datenkommunikationen zwischen Nutzern durch kryptographische Verfahren.

HINTERGRUND

[0002] Kryptographische Implementierungen können als Suites ausgeführt werden, die verfügbar sind, um von einer Vielzahl von Computerprogrammen (auch als Anwendungen bezeichnet) aufgerufen zu werden. Verschiedene Applikationen rufen kryptographische Operationen bei der Speicherung und Kommunikation von Daten auf. Die Verschlüsselungsoperationen werden durch verschiedene Verschlüsselungsverfahren, -Protokolle und -Suites umgesetzt.

[0003] In Bereichen mit sensiblen Daten ist es für zwei oder mehrere Anwendungen eine bewährte Verfahrensweise, Daten untereinander unter Verwendung eines kryptographischen Verfahrens zu kommunizieren. Die Wahl des kryptographischen Verfahrens hängt von vielen Faktoren ab: einschliesslich Verarbeitungslast, Fehlerkontrolle, Authentifizierung, Nachweisbarkeit, Kenntnis und Vertrauen hinsichtlich der anderen Anwendung usw. Ein anderer Faktor ist, ob das kryptographische Verfahren in dem Rechtssystem, in welchem die Anwendung verwendet wird, verfügbar oder geläufig ist. In einigen Fällen werden in verschiedenen Rechtssystemen aus verschiedenen Gründen bestimmte kryptographische Verfahren oder Suites favorisiert oder durchgesetzt und es ist nicht ungewöhnlich, dass verschiedene Länder in verbreiteten Industrien verschiedene kryptographische Verfahren durchsetzen. Bei diesen Beispielen kann es schwierig sein, Daten sicher zwischen Unternehmen in unterschiedlichen Ländern auszutauschen, die in diesen Industrien tätig sind.

[0004] Zudem werden kryptographische Implementierungen durch Anwendungen aufgerufen, deren zugrunde liegende Quellcodesprachen und Architekturen voneinander abweichen und welche auf zahlreichen Plattformen und Gerätetypen agieren. Diese Anwendungen müssen jedoch mit Anwendungen kommunizieren, die auf verschiedenen Plattformen und mit verschiedenen Codesprachen gehostet werden.

[0005] Sensible Daten werden vermehrt über ungesicherte Netzwerke übertragen, während die Vielfalt von Anwendungen weiterhin wächst. Zusätzlich gibt es bei einer Vielzahl von Providern eine grössere Vielfalt von kryptographischen Implementierungen, die darauf ausgerichtet sind, übertragene Daten vor einem Abfangen zu schützen.

ZUSAMMENFASSUNG

[0006] In einem Aspekt wird ein Verfahren für das kryptographische Suite-Management bereitgestellt, wobei das Verfahren Folgendes umfasst: Konfigurieren eines ersten Korrespondenten, der mit einer ersten kryptographischen Suite-Management-Einheit verbunden ist, um eine Importanfrage an einen zweiten Korrespondenten zu übertragen, der mit einer zweiten kryptographischen Suite-Management-Einheit verbunden ist, wobei die Anfrage die Identifizierung einer kryptographischen Implementierung und Sicherheitsanforderungen für die kryptographische Implementierung für den Export durch den zweiten Korrespondenten umfasst; Konfigurieren einer zweiten kryptographischen Suite-Management-Einheit, um die kryptographische Implementierung bereitzustellen, die unter Verwendung der Sicherheitsanforderungen konfiguriert wurde; Konfigurieren des zweiten Korrespondenten, um die konfigurierte kryptographische Implementierung zu dem ersten Korrespondenten zu exportieren; und Konfigurieren der ersten kryptographischen Suite-Management-Einheit, um die konfigurierte kryptographische Implementierung für die Verwendung durch den ersten Korrespondenten sicher zu importieren.

[0007] In einem anderen Aspekt wird ein System für das kryptographische Suite-Management bereitgestellt, wobei das System einen zweiten Korrespondenten umfasst, der mit einer zweiten kryptographischen Suite-Management-Einheit verbunden ist, die konfiguriert ist, um mit einem ersten Korrespondenten zu kommunizieren, der mit einer ersten kryptographischen Suite-Management-Einheit verbunden ist, wobei nach Übertragung einer Importanfrage durch den ersten Korrespondenten an den zweiten Korrespondenten gestellt wird, wobei die Anfrage die Identifizierung einer kryptographischen Implementierung und Sicherheitsanforderungen für die kryptographische Implementierung für den Export durch den zweiten Korrespondenten umfasst, die zweite kryptographische Suite-Management-Einheit konfiguriert ist, um die kryptographische Implementierung bereitzustellen, die unter Verwendung der Sicherheitsanforderungen konfiguriert wurde und die konfigurierte kryptographische Implementierung zu dem ersten Korrespondenten zu exportieren, um es der ersten kryptographischen Suite-Management-Einheit zu ermöglichen, die konfigurierte kryptographische Implementierung für die Verwendung durch den ersten Korrespondenten sicher zu importieren.

[0008] In einem anderen Aspekt wird ein System für das kryptographische Suite-Management bereitgestellt, wobei das System eine kryptographische Suite-Management-Einheit umfasst, die konfiguriert ist, um kryptographische Funktionen unter Verwendung kryptographischer Provider-Implementierungen aus einer kryptographischen Bibliothek als Reaktion auf einen Abruf von einer Anwendung auszuführen, wobei die kryptographische Suite-Management-Einheit ferner konfiguriert ist, um eine oder mehrere der kryptographischen Provider-Implementierungen zur Verwendung durch eine Drittpartei auszutauschen.

[0009] In den Ausführungsformen werden Systeme und Verfahren bereitgestellt, um den Austausch und die Verwendung von kryptographischen Suites zwischen Anwendungen und Geräten zu ermöglichen.

[0010] In weiteren Ausführungsformen werden Systeme und Verfahren bereitgestellt, um es einem kryptographischen Suite-Management zu ermöglichen, eine Vielzahl kryptographischer Provider-Suites für verschiedene Anwendungen und Geräte über eine Anzahl von Plattformen verfügbar zu machen.

[0011] In noch weiteren Ausführungsformen werden Systeme und Verfahren bereitgestellt, um den Import/Export von kryptographischen Suites zwischen Anwendungen und Geräten zu ermöglichen.

[0012] In noch weiteren Ausführungsformen werden Systeme und Verfahren für das Umschreiben von Daten zwischen Geräten, die verschiedene kryptographische Implementierungen aufrufen, bereitgestellt.

[0013] In noch weiteren Ausführungsformen werden Systeme und Verfahren für die Durchsetzung von Richtlinien bereitgestellt, welche die Nutzungsbedingungen für kryptographische Suites bestimmen, die zwischen Anwendungen und Geräten verwendet oder ausgetauscht werden.

[0014] In noch weiteren Ausführungsformen werden Systeme und Verfahren zum Schutz kryptographischer Suites bereitgestellt, die zwischen Anwendungen und Geräten ausgetauscht werden.

[0015] In noch weiteren Ausführungsformen werden Systeme und Verfahren zur Festlegung und Verwaltung von Richtlinien bereitgestellt, welche die Nutzungsbedingungen für kryptographische Suites bestimmen, die zwischen Anwendungen und Geräten verwendet oder ausgetauscht werden.

[0016] Diese und andere Ausführungsformen werden hierin betrachtet und beschrieben. Es wird gewürdigt, dass die vorstehende Zusammenfassung repräsentative Aspekte von Systemen und Verfahren für das kryptographische Suite-Management darlegt, um sachkundigen Lesern beim Verständnis der folgenden detaillierten Beschreibung zu helfen.

BESCHREIBUNG DER ZEICHNUNGEN

[0017] Ein umfassenderes Verständnis der Ausführungsformen wird mit Bezug auf die Figuren möglich, bei denen:

Fig. 1 eine Konfiguration eines Systems für das kryptographische Suite-Management veranschaulicht;

Fig. 2 APIs für eine Ausführungsform einer kryptographischen Suite-Management-Einheit veranschaulicht;

Fig. 3 ein Verfahren für den freigegebenen Import einer kryptographischen Provider-Suite veranschaulicht;

Fig. 4 ein Verfahren für den blockierten Import einer kryptographischen Provider-Suite veranschaulicht;

Fig. 5 eine kryptographische Suite-Management-Einheit in einer eng gekoppelten Ausführungsumgebung veranschaulicht;

Fig. 6 eine kryptographische Suite-Management-Einheit in einer verteilten Ausführungsumgebung veranschaulicht;

Fig. 7 eine kryptographische Suite-Management-Einheit veranschaulicht, die in einer C- und Java-Programmumgebung konfiguriert ist;

Fig. 8 das dynamische Laden einer kryptographischen Provider-Implementierung veranschaulicht;

Fig. 9 die Abstraktion eines plattformspezifischen dynamischen Ladens in der kryptographischen Suite-Management-Einheit veranschaulicht;

Fig. 10 ein Verfahren zum Laden und Speichern eines Suite-Tresors veranschaulicht;

Fig. 11 ein Verfahren für das Entladen einer kryptographischen Provider-Implementierung veranschaulicht;

Fig. 12 ein Verfahren zum Erzeugen kryptographischer Provider-Pakete veranschaulicht;

Fig. 13 eine Bündelungs- und Verschlüsselungskonfiguration veranschaulicht;

Fig. 14 eine andere Bündelungskonfiguration veranschaulicht;

Fig. 15 ein Verfahren zum Importieren von Paketen veranschaulicht;

Fig. 16 ein Verfahren zum Bündeln einer lizenzpflichtigen kryptographischen Provider-Implementierung veranschaulicht;

Fig. 17 ein Verfahren zum sicheren Speichern von Schlüsseln veranschaulicht;

Fig. 18 ein anderes Verfahren zum sicheren Speichern von Schlüsseln veranschaulicht;

Fig. 19 ein Verfahren zum Laden und Speichern eines Suite-Tresors veranschaulicht;

Fig. 20 ein Verfahren für das Entladen einer kryptographischen Provider-Implementierung veranschaulicht;

Fig. 21 ein Verfahren zum Abrufen kryptographischer Provider-Implementierungen in einem Hardware-Suite-Tresor veranschaulicht;

Fig. 22 ein Verfahren zum sicheren Speichern einer kryptographischen Suite in einem Hardware-Suite-Tresor veranschaulicht;

Fig. 23 ein Verfahren zum Registrieren einer Anwendung mit einem Hardware Secure Module veranschaulicht;

Fig. 24 eine Konfiguration für die kryptographische Abstraktion veranschaulicht;

Fig. 25 eine Konfiguration für die Überschreibung veranschaulicht;

Fig. 26 ein Verfahren für die Überschreibung veranschaulicht; und

Fig. 27 ein Verfahren für die Verwaltung einer Vielzahl von Instanzen für kryptographische Suite-Management-Einheiten, kryptographische Provider-Implementierungen und Richtlinien veranschaulicht.

DETAILLIERTE BESCHREIBUNG

[0018] Es wird gewürdigt, dass die Referenzziffern, wenn als angemessen erachtet, im Sinne der Einfachheit und Klarheit der Veranschaulichung in den Figuren wiederholt werden können, um zugehörige oder analoge Elemente zu kennzeichnen. Zusätzlich werden zahlreiche spezifische Details dargelegt, um ein umfassendes Verständnis der hierin beschriebenen Ausführungsformen zu ermöglichen. Für einen durchschnittlichen Fachmann versteht es sich jedoch, dass die hierin beschriebenen Ausführungsformen ohne diese spezifischen Details umgesetzt werden können. In anderen Fällen wurden wohlbekannte Methoden, Verfahren und Komponenten nicht ausführlich beschrieben, damit die hierin beschriebenen Ausführungsformen nicht unklar werden. Ebenso soll die Beschreibung nicht als Einschränkung hinsichtlich des Umfangs der hierin beschriebenen Ausführungsformen angesehen werden.

[0019] Es wird gewürdigt, dass verschiedene Begriffe, die im Zuge der vorliegenden Beschreibung verwendet werden, wie folgt gelesen und verstanden werden können, sofern durch den Kontext nicht etwas anderes angegeben wird: «oder», wie es hier verwendet wird, ist inklusiv, als ob «und/oder» geschrieben wäre; Artikel im Singular und Pronomen, wie sie hier verwendet werden, schliessen ihre Pluralformen mit ein und umgekehrt; gleichermassen schliessen Geschlechtspronomen Pronomen, die ihr Gegenstück darstellen, mit ein, sodass Pronomen nicht als Einschränkung für etwas verstanden werden sollten, das hierin in Bezug auf Verwendung, Umsetzung, Leistung usw. durch ein einzelnes Geschlecht beschrieben wird. Weitere Begriffsdefinitionen können hierin dargelegt werden; diese können für vorhergehende und nachfolgende Beispiele dieser Begriffe gelten, was durch das Lesen der vorliegenden Beschreibung verstanden wird.

[0020] Es wird gewürdigt, dass sämtliche Module, Einheiten, Komponenten, Server, Computer, Terminals oder Geräte, die hierin erläutert werden und Anweisungen ausführen, computerlesbare Medien wie Speichermedien, elektronische Speichermedien oder Datenspeichervorrichtungen (entfernbar und/oder nicht entfernbar) wie zum Beispiel Magnet-Disks, optische Speicherplatten oder Band umfassen oder anderweitig Zugang zu solchen Medien haben können. Elektronische Speichermedien können flüchtige und nicht flüchtige, entfernbare und nicht entfernbare Medien umfassen, die mit einem beliebigen Verfahren oder einer beliebigen Technologie zum Speichern von Informationen wie computerlesbaren Anweisungen, Datenstrukturen, Programmmodulen oder anderen Daten implementiert werden. Beispiele für elektronische Speichermedien umfassen RAM, ROM, EEPROM, Flash-Speicher oder andere Speichertechnologien, CD-ROM, Digital Versatile Disks (DVD) oder andere Möglichkeiten für die optische Speicherung, Magnetkassetten, Magnetband, die Speicherung auf Magnet-Disks oder anderen magnetischen Speichervorrichtungen oder jedes andere Medium, das verwendet werden kann, um die gewünschten Informationen zu speichern und auf welches eine Anwendung, ein Modul oder beide zugreifen kann bzw. können. Jedes derartige elektronische Speichermedium kann Teil des Geräts oder diesem zugänglich oder mit diesem verknüpfbar sein. Ferner, sofern durch den Kontext nicht etwas anderes angegeben wird, kann jeder hierin dargelegte Prozessor bzw. jede Steuereinheit als ein einzelner Prozessor oder als eine Vielzahl von Prozessoren implementiert werden. Die Vielzahl von Prozessoren kann geordnet oder verteilt sein und jede hierin angesprochene Verarbeitungsfunktion kann durch einen oder eine Vielzahl von Prozessoren ausgeführt werden, auch wenn ein einzelner Prozessor erläutert wurde. Sämtliche hierin beschriebenen Verfahren, Anwendungen oder Module können unter Verwendung computerlesbarer/-ausführbarer Anweisungen implementiert werden, die gespeichert oder anderweitig von solchen computerlesbaren Medien aufbewahrt und von dem einen oder mehreren Prozessoren ausgeführt werden können.

[0021] Das Folgende betrifft Datenkommunikationssysteme, die durch kryptographische Verfahren gesichert werden. In den Aspekten ermöglichen die folgenden Systeme und Verfahren die Kommunikation zwischen mehreren kryptographischen Korrespondenten (Nutzern) oder Anwendungen, die verschiedene kryptographische Suites von Verfahren verwenden.

[0022] In einem Aspekt werden hierin ein System und ein Verfahren beschrieben, die das Verwenden eines Protokolls umfassen, das den Export von einem Nutzer einer Implementierung einer kryptographischen Suite zu einem anderen Nut-

zer zum Import und dem dynamischen Laden der Implementierung ermöglichen. Das Verfahren umfasst ein Protokoll zum Verhandeln verschiedener Sicherheitsanforderungen für jeden der Nutzer und ihre Anwendungen; und das dynamische Laden der kryptographischen Suite durch den importierenden Nutzer.

[0023] In einem anderen Aspekt werden ein System und ein Verfahren beschrieben, bei denen ein vertrauenswürdiger Drittmittler eine sichere Kommunikation zwischen Nutzern und Anwendungen ermöglicht, wobei ein erster Nutzer bzw. eine Anwendung eine Datenquelle sein kann und ein zweiter Nutzer ein Datenempfänger sein kann. Die Drittpartei importiert die kryptographische Suite-Implementierung jedes Nutzers, verwendet die zu der Datenquelle gehörige Implementierung, um Chiffretexte von der Datenquelle zu entschlüsseln und verwendet dann die zu dem Datenempfänger gehörige Implementierung, um die Chiffre-Suites zu verschlüsseln. Diese Systeme und Verfahren sind Funktionen eines kryptographischen Suite-Management-Systems, das Folgendes ermöglicht: den Austausch und die Verwendung kryptographischer Implementierungen zwischen Nutzern und Anwendungen; für Anwendungen das dynamische Laden und die Verwendung kryptographischer Algorithmen auf sichere Weise; die Durchsetzung von Richtlinien, die mit der Verwendung einer oder mehrerer kryptographischer Suites verbunden sind; die sichere Kommunikation zwischen Nutzern oder Anwendungen, die verschiedene kryptographische Algorithmen unterstützen; und das Verwalten von kryptographischen Suites und den damit verbundenen Richtlinien.

[0024] In Bereichen mit sensiblen Daten ist es für zwei oder mehrere Anwendungen eine bewährte Verfahrensweise, Daten untereinander unter Verwendung eines kryptographischen Verfahrens zu kommunizieren. Die Wahl des kryptographischen Verfahrens hängt von vielen Faktoren ab: einschliesslich Verarbeitungslast, Fehlerkontrolle, Authentifizierung, Nachweisbarkeit, Kenntnis und Vertrauen hinsichtlich der anderen Anwendung usw. Ein anderer Faktor ist, ob das kryptographische Verfahren in dem Rechtssystem, in welchem die Anwendung verwendet wird, verfügbar oder geläufig ist. In einigen Fällen werden in verschiedenen Rechtssystemen aus verschiedenen Gründen bestimmte kryptographische Verfahren oder Suites favorisiert oder durchgesetzt.

[0025] In einer erläuternden Situation kann es im Interesse einer Bank liegen, einen sicheren Kommunikationskanal zwischen ihren Filialen in zwei verschiedenen derartigen Rechtssystemen (z. B. in zwei verschiedenen Ländern) herzustellen, wobei jedes Rechtssystem eine andere kryptographische Suite durchsetzt als das andere. Die Filialen in einem derartigen Rechtssystem können demnach eine andere kryptographische Suite verwenden als die Filialen der Bank in dem anderen Rechtssystem. Eine Herangehensweise, die durch eine oder mehrere der folgenden Ausführungsformen ermöglicht wird, wäre es, wenn eine andere Partei wie zum Beispiel die internationale Hauptverwaltung der Bank als ein Vermittler fungiert, um zwischen den Filialen in den verschiedenen Rechtssystemen unter Verwendung der kryptographischen Suite für die jeweiligen Filialen jedes Rechtssystems zu kommunizieren, um die Chiffretexte von einer kryptographischen Suite in die andere zu übersetzen.

[0026] In anderen Situationen werden kryptographische Implementierungen durch Anwendungen aufgerufen, deren zugrunde liegende Quellcodesprachen und Architekturen voneinander abweichen und welche auf zahlreichen Plattformen und Gerätetypen agieren. Diese Anwendungen müssen jedoch möglicherweise mit Anwendungen kommunizieren, die auf verschiedenen Plattformen und mit verschiedenen Codesprachen gehostet werden.

[0027] In noch anderen Situationen können sensible Daten zwischen verschiedenen Nutzern und Anwendungen unter Einsatz zahlreicher kryptographischer Implementierungen von einer Vielzahl von Providern über ungesicherte Netzwerke übertragen werden, sodass jeder Nutzer eine kryptographische Suite verwendet, die darauf ausgerichtet ist, die übertragenen Daten dieses Nutzers vor einem Abfangen zu schützen. Für Nutzer, die individuelle kryptographische Suites verwenden, die mit verschiedenen Verfahren, Parametern und Implementierungen konfiguriert sind, kann es wünschenswert sein, mit anderen Nutzern zu kommunizieren, während sie sich ihre individuellen kryptographischen Ressourcen zunutze machen. Für solche Nutzer kann die Unabhängigkeit, die durch individuelle kryptographische Ressourcen ermöglicht wird, wünschenswert sein, während sie von der Vernetzbarkeit mit anderen Nutzern profitieren. Eine Herangehensweise, die durch eine oder mehrere der folgenden Ausführungsformen ermöglicht wird, wäre für solche Nutzer der Austausch kryptographischer Suites miteinander oder der Einsatz einer Drittpartei zum Verwenden ihrer jeweiligen kryptographischen Suites, um einen sicheren Datenaustausch zwischen Nutzern zu vereinfachen.

[0028] Das Folgende stellt Systeme und Verfahren für das kryptographische Suite-Management bereit. Die hierin bereitgestellten Systeme und Verfahren für das kryptographische Suite-Management, ermöglichen eine Interoperabilität und sichere Kommunikation zwischen Anwendungen und Plattformen, die entweder gemeinsame oder verschiedene kryptographische Provider-Implementierungen oder -Suites aufrufen. Die Systeme und Verfahren für das kryptographische Suite-Management können ferner eine Vielzahl von Anwendungen ermöglichen, die in einem einzelnen Gerät oder auf einer einzelnen Plattform arbeiten, um auf eine Vielzahl von kryptographischen Provider-Implementierungen zuzugreifen. Die Systeme und Verfahren für das kryptographische Suite-Management können es ferner Anwendungen ermöglichen, kryptographische Provider-Implementierungen für andere Anwendungen zu bündeln oder zu exportieren. Die Systeme und Verfahren für das kryptographische Suite-Management können es ferner Anwendungen ermöglichen, kryptographische Provider-Implementierungen auf sichere Weise dynamisch zu laden und auszuführen. Die Systeme und Verfahren für das kryptographische Suite-Management können ferner die Durchsetzung von Richtlinien, welche die Nutzungsbedingungen für kryptographische Provider-Implementierung bestimmen, durch Anwendungen ermöglichen.

[0029] In Aspekten ermöglicht es eine kryptographische Suite-Management-Einheit einer Anwendung, kryptographische Funktionen aufzurufen, die von einer Vielzahl von kryptographischen Provider-Suites bereitgestellt werden.

[0030] Nun veranschaulicht in Bezug auf Fig. 1 ein Blockdiagramm ein System 100, das eine Anwendung 102 ausführt, die zum Abrufen von Verschlüsselungsfunktionen konfiguriert ist. Das System 100 kann mindestens eine solche Anwendung 102 (welche hierin als eine «Abrufanwendung» bezeichnet werden kann), ein Betriebssystem 104, ein Dateisystem 106, einen Speicher 108 und kryptographische Hardware 110 wie zum Beispiel ein Hardware Secure Module (HSM) umfassen. Diese Elemente kommunizieren mit einer kryptographischen Suite-Management-Einheit 112, welche die Anwendung und das Teilen – durch Import, Export und Lizenzierung – von einer oder mehreren kryptographischen Suites verwaltet.

[0031] Die kryptographische Suite-Management-Einheit 112 kann Folgendes umfassen: eine kryptographische API 114; eine API zur Schlüsselverwaltung 116; eine API zur Rechteverwaltung 118; eine OpenSSL-API 120; eine Protokoll-API 122; eine API zur Providerregistrierung 124; eine API zur Konfigurationsverwaltung 126; ein Warnmodul 128; ein Protokollmodul 130; einen Konfigurationsmanager 132; einen Chiffre-Suite-Tresor 134 zum sicheren Speichern von kryptographischen Provider-Suites; einen Schlüsseltresor 136 zum sicheren Speichern kryptographischer Schlüssel; ein Import-/Exportmittel 138 zum Importieren und/oder Exportieren kryptographischer Provider-Pakete; ein Richtlinienmittel 140 zum Verwalten der Verteilung von Richtlinien, welche die Nutzungsbedingungen für kryptographische Provider bestimmen; einen Richtlinienserver 142 zum zentralen Verwalten von Richtlinien und kryptographischen Providern in einer Sicherheitsdomäne; einen Container-Client 144 zum Zugriff auf kryptographische Provider-Pakete und Schlüssel in dem Suite-Tresor und dem Schlüsseltresor; einen Hardware-Client 146 zur Kommunikation mit kryptographischer Hardware; und eine Providerregistrierungskomponente 124 zum Registrieren kryptographischer Provider mit der kryptographischen Suite-Management-Einheit. Das Betriebssystem 104 kommuniziert mit dem Dateisystem 106 und dem Speicher 108. Die jeweilige Funktion jeder dieser Komponenten wird hierin beschrieben.

[0032] In weiteren Aspekten ermöglicht die kryptographische Suite-Management-Einheit 112 den Import, den Austausch und die Verwendung einer Vielzahl von kryptographischen Provider-Suites zwischen Geräten und Anwendungen. Der Austausch von kryptographischen Provider-Suites zwischen Geräten kann über eine Netzwerkverbindung zwischen den Geräten eingerichtet werden; üblicherweise über das Internet, wie aus Fig. 27 ersichtlich.

[0033] Durch den Import von mehr als einer kryptographischen Provider-Suite auf ein Gerät können andere Anwendungen auf dem Gerät auf eine oder mehrere der Vielzahl von kryptographischen Provider-Suites zugreifen, um Daten zu verschlüsseln und/oder zu entschlüsseln oder um andere kryptographische Operationen auszuführen. Die Import-/Exportoperation wird durch ein Protokoll festgelegt, das konfiguriert ist, um sowohl die Anforderungen der Importer als auch der Exporter zu verhandeln, ohne die Sicherheit der zugrunde liegenden Anwendungen zu vermindern.

[0034] Die kryptographische Suite-Management-Einheit 112 kann eine Suite von APIs wie zum Beispiel eine API für die Chiffre-Verwaltung 148, eine API zur Konfigurationsverwaltung 126, eine Schlüsseltresor-API 150 und eine Suite-Tresor-API 152 umfassen, die mit dem Import und Export von Chiffre-Suites, wie in Fig. 2 veranschaulicht, verknüpft ist.

[0035] Die API für die Chiffre-Verwaltung 148 (als «CipherMgtApi» veranschaulicht) stellt Funktionen bereit, die zur Verwaltung kryptographischer Provider-Pakete, umfassend die folgenden Beispiele für die kryptographische Suite-Management-Einheit, verwendet werden, um Export- und Importoperationen für Chiffre-Suite-Pakete auszuführen:

- «Importanfrage» 154 ist eine Anfrage durch einen Importer, um einen kryptographischen Provider mit einem festgelegten Sicherheitsniveau und spezifizierten Plattforminformationen zu erhalten. Die Anfrage umfasst einen Public Key, der von dem Importer generiert wird, um für die Verschlüsselung des kryptographischen Providers verwendet zu werden; das heisst, dass der kryptographische Provider an sich sicher mit der anfragenden Partei geteilt werden kann;
- «ImportanfrageBekommen» 156 ist eine Antwort von einem Exporter als Reaktion auf und nach einer Analyse einer Importanfrage. Der Exporter empfängt die Informationen von der Importanfrage, bestimmt das Sicherheitsniveau seiner Anwendung und sucht seinen Tresor nach einem passenden kryptographischen Provider ab. Auf der Grundlage von Import-/Exportrichtlinien eines passenden kryptographischen Providers bestimmt der Exporter, ob er den passenden kryptographischen Provider exportieren soll. Der Name dieses kryptographischen Providers wird an die Anwendung geliefert. Dies ist die einzige Information, die von einer Anwendung, die in einer kryptographischen Suite-Management-Einheit integriert ist, benötigt wird, um den kryptographischen Provider zu verarbeiten;
- «Exportpaket»» 158 erzeugt eine Datei, die von einem kryptographischen Provider ausführbare Binärdateien und Richtlinien enthält, welche die Nutzungsbedingungen bestimmen, die exportiert und für die Verwendung durch eine andere Anwendung ausgeliehen werden können. In einer Ausführungsform umfasst diese Operation die folgenden Schritte:
  - Empfangen des Public Keys eines Importers, der für den Zweck der Exportoperation generiert wurde;

- Erzeugen einer kryptographischen Paketdatei mit Headerfeldern, die mit geeigneten Werten gemäss den Details der Anfrage befüllt sind;
- Erzeugen einer zugehörigen Lizenzdatei mit den notwendigen Daten für Richtlinien und die Sicherheit;
- Generieren, falls erforderlich, eines Schlüsselpaars, das zum Verschlüsseln des kryptographischen Provider-Pakets wird;
- Verschlüsseln des kryptographischen Provider-Pakets unter Verwendung des Public Keys des Importers und, falls nötig, des Private Keys des Exporters;
- Archivieren des verschlüsselten kryptographischen Provider-Pakets, der Lizenzdatei und der Public-Keys, welche der Funktion in einem einzelnen Archiv wie zum Beispiel einem Zip- oder Tarball-Archiv bereitgestellt werden.

• «Paketimportieren» 160 führt die Importoperationen innerhalb einer Anwendung aus, die ein exportiertes kryptographisches Provider-Paket empfängt. In einer Ausführungsform umfasst diese Operation die folgenden Schritte:

- Extrahieren des verschlüsselten kryptographischen Provider-Pakets, der Lizenzdatei und der Public Keys aus dem Archiv;
- Validieren der Dateiintegrität;
- Verwenden des geeigneten Public Keys aus dem Archiv, um den zugehörigen Private Key zu suchen;
- Entschlüsseln des kryptographischen Provider-Pakets unter Verwendung des Public Keys des Exporters und, falls nötig, des Private Keys des Importers;
- Validieren der Dateiheader und -integrität;
- Speichern des kryptographischen Provider-Pakets in dem Suite-Tresor; und
- Registrieren des kryptographischen Provider-Pakets mit dem Konfigurationsmanager zum Laden, um kryptographische Operationen auszuführen.

[0036] Es wird von einem Fachmann gewürdigt werden, dass die Namen, die mit den vorstehenden (oder beliebigen folgenden) Funktionen verbunden sind, auf gewünschte Weise modifiziert werden können.

[0037] Die API zur Konfigurationsverwaltung 126 (veranschaulicht als «ConfigMgrApi») stellt Funktionen zur Verwaltung der Konfiguration der kryptographischen Suite-Management-Einheits-Konfiguration bereit, umfassend die folgenden Beispiele zum Registrieren und zum Aufheben der Registrierung von Paketen, die zur Durchführung von kryptographischen Operationen verfügbar sind:

• «PaketRegistrieren» 162 speichert Informationen in Bezug auf ein Paket, das in den Suite-Tresor importiert wurde;

• «PaketEntfernen» 164 löscht Informationen in Bezug auf ein Paket, das aus dem Suite-Tresor entweder als ein Ergebnis einer Benutzeraktion oder aufgrund von Lizenzbedingungen entfernt wurde; und

• «PaketeAuflisten» 166 schickt Informationen über alle in dem Suite-Tresor verfügbaren kryptographischen Provider-Suites zurück.

[0038] Die API zur Konfigurationsverwaltung 126 kann ebenso Funktionen bereitstellen, die zum Bereitstellen von Informationen an Abrufanwendungen und des Zugangs zu Diensten der kryptographischen Suite-Management-Einheit bei verschiedenen Sicherheitsniveaus, also verschiedenen Implementierungen, erforderlich sind. Jede Krypto-Provider-Implementierung ist mit einem kryptographischen Sicherheitsniveau ausgestattet. Dies ist ein Teil der Informationen, die der Exporter der Implementierung öffentlich machen muss.

[0039] Die Schlüsseltresor-API 150 (veranschaulicht als «KeyVaultApi») stellt Funktionen zur Verwaltung geheimer Schlüssel bereit, die von der kryptographischen Suite-Management-Einheit 112 benötigt werden, umfassend die folgenden Funktionsaufrufe zum Generieren von Schlüsselpaaren und zum Wiederherstellen von Schlüsseln, die benötigt werden, um Verschlüsselungs- und Entschlüsselungsoperationen auszuführen:

• «SchlüsselpaarGenerieren» 168 generiert ein asymmetrisches Schlüsselpaar und speichert den Private Key sicher in dem Schlüsseltresor. In dem Zusammenhang der Verwaltung von Chiffre-Suites wird dieser Abruf von der

empfangenden Anwendung gemacht, um ein KEK/KDK-Paar zu generieren und von der sendenden Anwendung, um das BEK/BDK-Paar zu generieren; und

- «PrivateKeyBekommen» 170 stellt einen Private Key aus dem Schlüsseltresor wieder her. In dem Kontext der Verwaltung von Chiffre-Suites macht die empfangende Anwendung diesen Abruf, um die Private Key-KDK wiederherzustellen, die mit der KEK verknüpft ist, die während Entschlüsselungsoperationen während des Importvorgangs benötigt wird.

[0040] Die Suite-Tresor-API 152 stellt Funktionen zum Verwalten kryptographischer Provider-Suites bereit, die in dem Suite-Tresor gespeichert sind, umfassend Support für die folgenden Operationen:

- «PaketSpeichern» 172 speichert dauerhaft ein kryptographisches Provider-Paket in verschlüsseltem Format;
- «PaketEntfernen» 174 entfernt dauerhaft und sicher ein kryptographisches Provider-Paket aus dem dauerhaften Speicher;
- «PaketLaden» 176 liest ein kryptographisches Provider-Paket aus dem dauerhaften Speicher, entschlüsselt das kryptographische Provider-Paket und verbindet das kryptographische Provider-Paket dynamisch mit der laufenden Operation zur Verwendung bei der Ausführung kryptographischer Operationen;
- «PaketEntladen» 178 trennt das entschlüsselte Paket von der laufenden Anwendung und entfernt sicher den unverschlüsselten Code und die Daten, die mit dem kryptographischen Provider-Paket verknüpft sind, aus dem flüchtigen und nicht flüchtigen Speicher; und
- «PaketeValidieren» 180 wird von der kryptographischen Suite-Management-Einheit aufgerufen, wenn es zum Überprüfen und Anwenden der Richtlinien für die verschiedenen in dem Suite-Tresor gespeicherten Pakete, wie zum Beispiel einer Richtlinie zum sicheren Entfernen eines Pakets mit einer abgelaufenen Lizenz aus dem dauerhaften Speichermedium, erforderlich ist.

[0041] Bei der Verwendung ruft eine Abrufanwendung 102 die kryptographische Suite-Management-Einheit 112 auf, um eine neue kryptographische Provider-Suite, wie aus Fig. 3 und 4 ersichtlich, zu importieren. Bei einigen Plattformen kann ein Blockieren während des Importvorgangs Aspekte des Systems destabilisieren. Zum Beispiel können einige Plattformen von mobilen Geräten gegenüber Blockiervorgängen empfindlich sein. Daher kann die API zur Providerregistrierung 124 für einen blockierten oder freigegebenen Import von kryptographischen Suites, wie jeweils aus Fig. 3 und 4 ersichtlich, konfiguriert sein.

[0042] Nun wird in Bezug auf Fig. 3 ein asynchroner, d. h. nicht blockierender Import einer kryptographischen Suite 300 veranschaulicht. An Block 302 wird nach einer Nutzeranfrage über eine Anwendungsbenutzerschnittstelle oder automatisch als Ergebnis einer Anwendungslogik ein einzigartiger Anfrage-Token, der mit einem Aufruf an die API zur Providerregistrierung verknüpft ist, um die kryptographische Suite eines gegebenen kryptographischen Providers zu importieren, durch die kryptographische Suite-Management-Einheit an die Anwendung bereitgestellt. An Block 304 führt die kryptographische Suite-Management-Einheit dann verschiedene Operationen für die Validierung und den Import aus, um die kryptographische Suite zu importieren; währenddessen kann der einzigartige Anfrage-Token von der Anwendung verwendet werden, um operative Statusmeldungen über den Importvorgang anzufordern und um geeignete Massnahmen wie das Benachrichtigen von Anwendungsbenutzern durch eine Anwendungsbenutzerschnittstelle, Protokolldateien oder andere geeignete Verfahren zu ergreifen.

[0043] Bei dem blockierten Importverfahren 400, in Fig. 4 veranschaulicht, führt der Aufruf von der Anwendung an die API zur Providerregistrierung, der aus den an Block 402 ausgeführten Aktionen resultiert, nicht zu einer Antwort, bis Prozesse die von der kryptographischen Suite-Management-Einheit an Block 404 zur Verarbeitung der Importanfrage eingeleitet wurden, erfolgreich abgeschlossen wurden oder als fehlgeschlagen angesehen werden.

[0044] Der oben beschriebene Import kann während der Laufzeit einer Abrufanwendung auftreten. Während die Schnittstelle zwischen der Anwendung und der kryptographischen Suite-Management-Einheit bei der Laufzeit statisch sein kann, können sich die Schnittstelle zwischen der kryptographischen Suite-Management-Einheit und die unterstützten kryptographischen Suites dynamisch verändern, um das Hinzufügen oder die Wegnahme einer oder mehrerer kryptographischer Provider-Suites während der Laufzeit widerzuspiegeln. Demnach kann die kryptographische Suite-Management-Einheit gemäss den folgenden allgemeinen Herangehensweisen konfiguriert werden, um kryptographische Provider-Suites zu beteiligen, die bei der Laufzeit hinzugefügt werden: (1) ein Verknüpfungsmodell für die Laufzeit (dynamisch), bei welchem die Programmanweisungen der kryptographischen Provider-Suite (kryptographischer Code) durch die Verwendung einer gemeinsamen oder dynamischen Bibliothek eng mit der kryptographischen Suite-Management-Einheit verbunden sind; und (2) ein verteiltes Client-Server-Modell, bei weichem auf kryptographische Provider-Suite-Dienste über den Aufruf entfernter Methoden oder die Kommunikation zwischen Prozessen zugegriffen wird.

[0045] Nun wird in Bezug auf Fig. 5 eine Ausführungsform 500 gezeigt, die unter Verwendung der Herangehensweise für die Laufzeitverknüpfung umgesetzt wird. Die Herangehensweise für die Laufzeitverknüpfung kann gegenüber dem verteilten Modell eine relativ verbesserte Leistung und Sicherheit bereitstellen, da die Anwendung 102, die kryptographische Suite-Management-Einheit 112 und die kryptographischen Provider-504-Implementierungen alle in der gleichen Anwendungsausführungsumgebung 502 ausgeführt werden. Es kann jedoch zwischen den Mechanismen, die auf verschiedenen unterstützten Plattformen verfügbar sind, für dynamische Verknüpfungskomponenten oder Bibliotheken eine signifikante Abweichung vorliegen, wodurch eine Implementierung von Plattform- und sprachspezifischem Code erforderlich wird.

[0046] In Bezug auf Fig. 6 kann eine Ausführungsform 600, die mit einem verteilten Modell umgesetzt wird, das den Aufruf entfernter Methoden oder die Kommunikation zwischen Prozessen 602 nutzt, was die dynamische Verknüpfung angeht, die plattform-und sprachspezifischen Abhängigkeiten reduzieren, obwohl signifikante Unterschiede zwischen unterstützten Plattformen immer noch für jede Plattform im Hinblick auf Optionen für das Threading, die Kommunikation zwischen Prozessen und den Aufruf entfernter Methoden ein Mass an Anpassung von Codes erforderlich machen können. Die Nachteile im Hinblick auf die Leistung und Sicherheit des verteilten Modells, die durch die Tatsache zustande kommen, dass die Anwendung 102 und die kryptographischen Provider 608 in unterschiedlichen Ausführungsumgebungen 604, 606 ausgeführt werden, können zumindest teilweise durch die Implementierung eines geeigneten Prozess- / Threading-Modells und eines Sicherheitsmechanismus abgeschwächt werden. Dies umfasst den Support für ein Modell für den Aufruf entfernter Methoden mit Multi-Thread oder Multi-Prozess, um die parallele Ausführung mehrerer kryptographischer Operationen, die Verwendung der gegenseitigen Authentifikation zwischen Kommunikationsprozessen und die Verwendung von Verschlüsselung für jegliche Kommunikation zwischen Prozessen zu ermöglichen.

[0047] Bestimmte Anwendungen oder Komponenten davon, welche die kryptographische Suite-Management-Einheit verwenden, können unter Verwendung verschiedener Programmiersprachen wie zum Beispiel Java, C oder C++ geschrieben werden. In einer Ausführungsform umfasst die kryptographische Suite-Management-Einheit eine C-basierte API, welche Anwendungen, die in C oder C++ geschrieben sind, nativ aufrufen kann, mit gleichwertigen API-Wrappern für andere Programmiersprachen.

[0048] Die kryptographische Suite-Management-Einheit 112 kann gemäss einem eng gekoppelten Modell, wie in Fig. 7 gezeigt, konfiguriert sein und sowohl Java-basierte Anwendungen 702 als auch C/C++-basierte Anwendungen/Komponenten 704 unterstützen. Da die API der kryptographischen Suite-Management-Einheit bei einer solchen Konfiguration sowohl für C als auch für Java-basierte Anwendungen verfügbar sein muss, wird die kryptographische Provider-Suite in C kodiert, sodass: C-Komponenten der aufrufenden Anwendung kryptographische Provider-Funktionen ohne Umwandlung aufrufen können; während Java-Komponenten einer aufrufenden Anwendung Aufrufe über eine Java-API 706 tätigen, welche Java Native Interface (JNI) verwenden, um auf die Funktionalität der C-basierten kryptographischen Provider-Suites zuzugreifen. Alle Java-Anwendungskomponenten, die mit der kryptographischen Suite-Management-Einheit interagieren, können dies über die Klassen der Java-API 706 für die kryptographische Suite-Management-Einheit tun. Die Java-API-Klassen sind einfache Wrapper, die JNI verwenden, um die benötigte Funktionalität durch die zugehörige C-API-Schnittstelle 708 aufzurufen.

[0049] In C 704 geschriebene Anwendungen oder Komponenten können mit der kryptographischen Suite-Management-Einheit 112 unter Verwendung der verfügbaren C-API 708 für die kryptographische Suite-Management-Einheit 112 interagieren. Die C-API 708 stellt wiederum Verknüpfungen mit dem Rest der eng gekoppelten (d. h. statisch verknüpft) Komponenten der kryptographischen Suite-Management-Einheit unter Verwendung nativer Funktionsaufrufe her.

[0050] Die kryptographische Suite-Management-Einheit kann konfiguriert sein, um auf einer Vielzahl von Plattformen, die unter anderem Android, iOS, MAC OS, Windows oder ein Linux-basiertes OS umfassen, betrieben zu werden. Diese Plattformen sind üblicherweise gebündelt oder können mit Implementierungen üblicher kryptographischer Suites gebündelt werden und eine Reihe kryptographischer APIs und Protokolle höherer Schichten (SSL, HTTPS) bereitstellen, die von Anwendungen verwendet werden können, die auf diesen Plattformen ausgeführt werden. Zusätzlich zur Bereitstellung dieser APIs an Anwendungen verwendet das OS an sich diese kryptographischen Implementierungen, um Eigenschaften wie die Dateisystemverschlüsselung bereitzustellen.

[0051] Ein Nutzer einer Anwendung, die auf einer standardmässigen Plattform ausgeführt wird, kann ein Aufrufen der kryptographischen Suite-Management-Einheit bevorzugen, um eine anwendereigene, kundenspezifische oder anderweitig nicht verfügbare Verschlüsselung von kryptographischen Providern unabhängig von kryptographischen Suites aufzurufen, die automatisch in dem OS bereitgestellt werden. Da die Sicherheitsmerkmale standardmässiger Betriebssysteme nicht zwangsläufig verlässlich sein müssen, kann die kryptographische Suite-Management-Einheit konfiguriert sein, um all ihre Daten zu schützen, die unter anderem kryptographische Provider-Pakete, Verschlüsselungsschlüssel und Daten in Bezug auf Konfiguration und Richtlinien umfassen, ohne sich auf die vorgegebenen Verschlüsselungseigenschaften des OS, wie hierin ausführlicher beschrieben, zu verlassen.

[0052] Die verschiedenen Plattformen, auf denen die kryptographische Suite-Management-Einheit konfiguriert sein kann, um Mechanismen bereitzustellen, die es Programmen, die auf diesen Plattformen ausgeführt werden, zu ermöglichen, Programmkomponenten dynamisch zu laden und auszuführen, die von den Anwendungen, welche sie aufrufen unabhängig sind. Beispiele für diese Fähigkeit umfassen unter anderem die DL-API, die für Linux und Mac OS verfügbar ist, das Run-Time Dynamic Linking von Microsoft, das für Windows verfügbar ist und das dynamische Verknüpfen für iOS

und Android. Wenn Komponenten der kryptographischen Suite-Management-Einheit kryptographische Provider-Verfahren aufrufen, kann eine Fähigkeit der zugrunde liegenden Plattform für die dynamische Verknüpfung genutzt werden. Dies ermöglicht, dass mehrere kryptographische Provider und von Providern geteilte Bibliotheken für die Verwendung durch die Anwendung bei der Laufzeit hinzugefügt und entfernt werden können, wenn sie nicht länger benötigt werden, wie hierin ausführlicher beschrieben.

[0053] In einer Ausführungsform kann sich die in Fig. 8 veranschaulichte Architektur für Linux ein generisches Potential von Linux für das dynamische Laden zunutze machen, welches für Linux-Plattformen im Allgemeinen zutreffend ist. Es wird gewürdigt werden, dass dynamisch geladenen (DL) Bibliotheken die übliche Herangehensweise für die Implementierung von Plug-ins oder Modulen in Linux-basierten Anwendungen wie zum Beispiel den Pluggable Authentication Modules (PAM) Systemen sind.

[0054] Die DL-API 802 stellt eine Reihe von Funktionen bereit, die es einer Anwendung ermöglichen, eine Bibliothek bei der Laufzeit dynamisch zu laden und Funktionen, die durch die Bibliothek bereitgestellt werden auszuführen. Fig. 8 veranschaulicht eine exemplarische Verwendung der Linux DL API durch eine Anwendung zum Laden und Ausführen von Code aus einer gemeinsamen Bibliothek. Der folgende Code-Ausschnitt veranschaulicht die Verwendung der Linux DL API:

```
#include <stdlib.h>

#include <stdio.h>

#include <dlfcn.h>

int main(int argc, char **argv) {

        void *handle;

        int (*encrypt)(char *dataIn, char (dataOut);

        char *error;

        char *dataToEncrypt[];

        char *encryptedData[];

        int result;


        handle = dlopen("/lib/provider1.so", RTLD_LAZY);
```

```
        if (!handle) {
                fputs (dlerror(), stderr);
                exit(1);
        }
        cosine = dlsym(handle, "encrypt");
        if ((error = dlerror()) != NULL) {
                fputs(error, stderr);
                exit(1);
        }

        result = (*encrypt)(dataToEncrypt, encryptedData));
        dlclose(handle);
}
```

[0055] Die DL-API 802 ist auf verschiedenen Linux-Plattformen, gelegentlich unter unterschiedlichen Namen wie zum Beispiel shl_load anstelle von dlopen verfügbar. Ferner sind bei anderen Betriebssystemen wie zum Beispiel Mac OS, iOS, Android und Windows analoge Mechanismen verfügbar. Daher umfasst die kryptographische Suite-Management-Einheit vorzugsweise eine Abstraktionsschicht 902, wie aus Fig. 9 ersichtlich, um ein plattformunabhängiges dynamisches Laden von Bibliotheken bereitzustellen, die kryptographische Provider-Funktionen enthalten.

[0056] Die Verwendung von dynamischen Verknüpfungseigenschaften für generische OS muss genutzt werden, um zu ermöglichen, dass kryptographische Provider-Implementierungen zwischen Instanzen kryptographischer Suite-Management-Einheiten ausgetauscht und bei der Laufzeit dynamisch geladen werden, sodass die Algorithmen, die in den kryptographischen Provider-Implementierungen enthalten sind, für die Anwendung verfügbar sind. Es wird gewürdigt, dass dynamische Verknüpfungseigenschaften für generische OS keine strikten Sicherheitsanforderungen angehen, die mit kryptographischen Provider-Implementierungen verbunden sind. Die kryptographische Suite-Management-Einheit kann Fähigkeiten bereitstellen, welche die dynamische Verknüpfung von kryptographischen Provider-Implementierungen ermöglichen, während Sicherheitsbedrohungen, die für kryptographische Implementierungen relevant sind, abgeschwächt werden.

[0057] Die dynamische Verknüpfung unter Verwendung standardmässiger OS-Eigenschaften macht es erforderlich, dass die zu verbindenden Module für das OS in unverschlüsseltem Format verfügbar sind, sodass die Programmanweisungen in den Systemspeicher geladen und für die Ausführung verfügbar gemacht werden können. Die Erzeuger oder Besitzer von kundenspezifischen kryptographischen Provider-Implementierungen können jedoch wünschen, dass die Algorithmen geheim bleiben, sodass die Speicherung der Bibliotheken im unverschlüsselten Format im nicht flüchtigen Speicher eine Sicherheitslücke darstellt, da die Algorithmen aus dem dauerhaften Speicher extrahiert und rekonstruiert werden könnten.

[0058] Um die Geheimhaltung kryptographischer Provider-Suites zu bewahren, kann ein sicherer Speichermechanismus wie zum Beispiel ein Suite-Tresor 134, wie in Fig. 1 veranschaulicht, bereitgestellt werden. Der Suite-Tresor kann als ein sicherer Hardware-basierter Container wie ein HSM- oder sicherer Speicher oder als ein Softwaremodul bereitgestellt werden, das die Funktionen bereitstellt, die für das Laden und Speichern kryptographischer Provider-Implementierungen nach Bedarf benötigt werden.

[0059] In einer Ausführungsform, die in Fig. 10 veranschaulicht wird, stellt der Suite-Tresor 134 ein Verfahren 1000 bereit, das es anderen Komponenten der kryptographischen Suite-Management-Einheit 112 ermöglicht, Operationen zum sicheren Speichern kryptographischer Provider-Pakete auszulösen und die kryptographischen Provider-Implementierungen zu einem späteren Zeitpunkt dynamisch zu laden, sodass die von ihr implementierten Algorithmen für die Anwendung verfügbar sind. Beim Speichern der kryptographischen Provider-Implementierung wird die Datei an Block 1002 unter Verwendung des kryptographischen Potentials der kryptographischen Suite-Management-Einheit verschlüsselt, Verschlüsselungsschlüssel werden sicher in dem Schlüsseltresor gespeichert und das verschlüsselte kryptographische Provider-Paket wird im dauerhaften Speicher bei Element 1005 gespeichert. Wenn eine Anwendung Funktionen dieses kryptographischen

Provider-Pakets aufrufen muss, wird es dynamisch mittels eines Aufrufs load_bundle an den Suite-Tresor, veranschaulicht als Element 1004, geladen. Als Reaktion auf diesen Aufruf erhält der Suite-Tresor den Schlüssel, der benötigt wird, um das kryptographische Provider-Paket aus dem Schlüsseltresor, veranschaulicht als Element 1006, zu entschlüsseln; lädt das verschlüsselte kryptographische Provider-Paket aus dem dauerhaften Speicher bei Element 1008; entschlüsselt die Datei des kryptographischen Provider-Pakets an Block 1008; löscht sicher die während des Entschlüsselungsvorgangs verwendeten Schlüssel aus dem Systemspeicher; schreibt die entschlüsselte Bibliotheksdatei des kryptographischen Provider-Pakets auf eine virtuelle Disk in dem flüchtigen Speicher bei Element 1010; verwendet die Abstraktionsschicht, um das zugrunde liegende Potential des Betriebssystems für die dynamische Verknüpfung aufzurufen, um das kryptographische Provider-Paket von der virtuellen Disk zu laden, wodurch die Funktionen für die Anwendung verfügbar gemacht werden. Die unverschlüsselte Datei des kryptographischen Provider-Pakets wird vorzugsweise so schnell wie möglich von der virtuellen Scheibe gelöscht und entfernt. Wenn die Anwendung nicht länger einen Zugriff auf die Funktionen der spezifischen kryptographischen Provider-Paket-Implementierung benötigt, benachrichtigt die kryptographische Suite-Management-Einheit den Suite-Tresor mittels eines Aufrufs close_bundle, veranschaulicht in Fig. 11 als Element 1102 gemäss einem Verfahren 1100. Als Reaktion auf diesen Aufruf leert der Suite-Tresor sicher den Speicher an der Stelle, wo die kryptographische Provider-Implementierung geladen wurde und verwendet die Abstraktionsschicht, um das zugrunde liegende Potential des OS für die dynamische Verknüpfung aufzurufen, um das Modul zu trennen.

[0060] Sobald ein kryptographischer Provider dynamisch mit der kryptographischen Suite-Management-Einheit verknüpft wurde, sind die Programmanweisungen und verknüpften Daten in dem Systemspeicher speicherresident, wo sie Modifikationen durch Programme unterzogen werden können, die ausreichend Zugriff auf solche Systemressourcen haben. Schadsoftware, die auf derselben Plattform ausgeführt werden kann wie der kryptographische Provider, kann dazu in der Lage sein, Programmanweisungen oder Daten zu modifizieren, wodurch die kryptographischen Algorithmen anfällig werden und die Daten freigeben, die sie schützen sollen. Die kryptographische Suite-Management-Einheit sichert die Integrität kryptographischer Provider-Implementierungen, die dynamisch geladen wurden, durch die Implementierung von Integritätsprüfungen für die geladenen Module. Wenn die Integritätsprüfungen eine Manipulation der Programmanweisungen des kryptographischen Providers oder der Daten feststellen, werden Informationen unter Verwendung des Protokollmoduls 130 der kryptographischen Suite-Management-Einheit aufgezeichnet, Anwendungen und Benutzer werden über das Warnmodul 128 gewarnt und weitere kryptographische Operationen können eingestellt werden, um die Preisgabe sensibler Informationen zu verhindern. Die kryptographische Suite-Management-Einheit 112 kann eine Anzahl von Verfahren für die Integritätsprüfung einsetzen, die unter anderem Folgendes umfassen: die Verwendung von Prüfsummenfunktionen, um zu verifizieren, dass Programmanweisungen nicht manipuliert wurden; die Verwendung von Testvektoren innerhalb des kryptographischen Suite-Providers, welche die Codeintegrität im Zusammenhang mit Metadaten verifizieren können, die in dem Krypto-Provider-Paket enthalten waren, als es in die kryptographische Suite-Management-Einheit importiert wurde; die Verwendung eines Challenge-Response-Protokolls zwischen der kryptographischen Suite-Management-Einheit und der kryptographischen Provider-Implementierung.

[0061] Wenn ein kryptographisches Provider-Paket zwischen zwei Instanzen der kryptographischen Suite-Management-Einheit ausgetauscht wird, kann die erzeugende Einheit die Richtlinien festlegen, welche die Nutzungsbedingungen des kryptographischen Suite-Providers bestimmen. Die empfangende kryptographische Suite-Management-Einheit setzt diese Richtlinien durch, um zu gewährleisten, dass die Verwendung des kryptographischen Suite-Providers durch die empfangende Anwendung mit den durch die erzeugende Einheit vorgeschriebenen Nutzungsbestimmungen übereinstimmt. Richtlinien können unter anderem Folgendes umfassen: das Betriebssystem, auf welchem die empfangende Einheit ausgeführt wird; die Verwendung eines Hardware-Suite-Tresors oder eines Software-Suite-Tresors durch die empfangende Einheit; die kryptographischen Algorithmen, die von der empfangenden Einheit verwendet werden, um den kryptographischen Provider zu schützen; die Grösse der von der empfangenden Einheit zum Schutz des kryptographischen Providers verwendeten Schlüssel; die Integritätsprüfungen, die von der empfangenden Einheit durchgeführt werden.

[0062] In Aspekten kann es die kryptographische Suite-Management-Einheit kryptographischen Providern ermöglichen, kryptographische Plug-ins für die Verteilung an mehrere verschiedene Plattformen zu bündeln und zu verteilen. Da eine einzelne Binärdatei für ein kryptographisches Plug-in nicht mit allen Plattformen, die von dem Plug-in unterstützt werden sollen, kompatibel sein kann, kann ein Packager aufgerufen werden, mehrere Binärdateien in einem Paket von Binärdateien zu bündeln, die konfiguriert sind, um mehrere Plattformen zu unterstützen. Das Paket von Binärdateien kann hierin als ein «kryptographisches Provider-Paket» 1202 bezeichnet werden. Die kryptographische Suite-Management-Einheit kann konfiguriert sein, um die Binärdatei bei der Laufzeit für die Plattform eines angestrebten Geräts eines Endnutzers zu importieren.

[0063] Der Packager 1204 bündelt die verteilbaren Informationen, die für eine spezifische kryptographische Provider-Implementierung erstellt wurden, in eine einzelne Datei, wie in Fig. 12 veranschaulicht.

[0064] Wie aus Fig. 13 ersichtlich, kann das kryptographische Provider-Paket 1302 Folgendes umfassen: einen generischen Header 1304, der Informationen über das Paket enthält, die seine Version und die Version der angestrebten kryptographischen Suite-Management-Einheit umfassen, um eine Kompatibilität zwischen der kryptographischen Suite-Management-Einheit, die das Paket importiert und der Provider-Implementierung zu gewährleisten; Sicherheitsmerkmale wie zum Beispiel eine Signatur 1306, um zu ermöglichen, dass importierende Anwendungen gewährleisten, dass (a) keine der verteilbaren Informationen verändert wurde, (b) das Paket von einer vertrauenswürdigen Packager-Anwendung erzeugt

wurde und (c) die Logik für die Lizenzierung und das Rechtemanagement für den importierten kryptographischen Provider angewendet werden kann; und (3) eine Reihe von Provider-Offsets 1308, welche die Grösse und den Ort jeder einzelnen verteilbaren Information festlegen, die in der Paketdatei enthalten ist.

[0065] Fig. 14 veranschaulicht im engeren Sinne die wesentlichen Headerfelder von Dateien, welche die Lizenzdatei 1406 und das kryptographische Provider-Paket 1404 umfassen können. Das kryptographische Provider-Paket 1404 kann die folgenden Header (denen nach Bedarf verschiedene Namen zugeordnet werden können) umfassen:

- «Generische Dateiinfo» 1408, welcher allgemeine kryptographische Suite-Informationen wie die Funktionen, die von dem Paket bereitgestellt werden, das unterstützte Sicherheitsniveau und Plattforminformationen enthalten kann;
- «Lizenzdateiinfo» 1410, welcher anzeigt, dass das Paket eine damit verbundene anwendungsspezifische Lizenz aufweist, d. h., dass es nicht für den allgemeinen Gebrauch durch eine nicht spezifizierte Anwendung gedacht ist. Das Feld identifiziert eindeutig die Lizenzdatei, die dem Paket zugeordnet ist. Wenn es frei gelassen wurde, kann die kryptographische Provider-Suite als offen angesehen werden, d. h. von jeder Anwendung importierbar, die von der kryptographischen Suite-Management-Einheit freigegeben wurde.
- «Krypto-Paket-ID» 1412, welcher eine eindeutige Bezeichnung eines Pakets ist, die verwendet werden kann, um eine Lizenzdatei einem spezifischen Paket zuzuordnen;
- «Lizenzdatei HMAC» 1414, welcher den Keyed-Hash Message Authentication Code (HMAC) der zugeordneten Lizenzdatei speichert; und
- «HMAC» 1416, welcher der HMAC des Pakets, einschliesslich aller Headerfelder ist, um eine Manipulation zu verhindern.

[0066] Die begleitende Lizenzdatei 1406 kann die folgenden Header umfassen:

- «Generische Headerinfo» 1418, welcher Informationen über die Lizenzdatei wie zum Beispiel die Dateiversion enthält;
- «Krypto-Paket-ID» 1420, welcher eine Bezeichnung ist, die das spezifische kryptographische Paket, welchem die Lizenzdatei zugeordnet ist, identifiziert;
- «Nutzungsrechte Info» 1422, welcher Informationen über die Nutzungsrechte des zugeordneten kryptographischen Pakets wie zum Beispiel Anfangs- und Enddatum oder Begrenzungen für abgelaufene Zeit enthält;
- «Empfänger-KEK» 1424, welcher einen Public Key identifiziert, der von dem Empfänger des Pakets bereitgestellt wird, das verwendet werden kann, um die notwendigen Schlüssel für die Entschlüsselung zu erhalten; und
- Kryptographische Metadaten 1426, die Informationen enthalten, die von der kryptographischen Suite-Management-Einheit-Operation benötigt werden.

[0067] Der Packager kann fermer konfiguriert sein, um eine verschlüsselte Paketdatei zu erzeugen. Jede verschlüsselte Paketdatei kann so verschlüsselt sein, dass sie nur durch den beabsichtigten Empfänger, wie hierin ausführlicher beschrieben, entschlüsselt werden kann.

[0068] Wie zuvor beschrieben und wie in Fig. 15 als Verfahren 1500 veranschaulicht, kann eine Anwendung 102 den Import eines neuen kryptographischen Provider-Pakets entweder automatisch oder als Ergebnis einer Benutzeraktion durch die Anwendungsbenutzerschnittstelle 1502 auslösen. Die Anwendung 102 ruft dann die kryptographische Suite-Management-Einheit 1504 auf, um das Paket zu verarbeiten. Die Datei wird an Block 1506 unter Verwendung der geeigneten Schlüssel (in einem anderen Szenario erörtert) entschlüsselt und die enthaltenen verteilbaren Informationen des Providers werden an Block 1508 extrahiert. An Block 1510 werden die geeigneten verteilbaren Informationen sicher in dem Suite-Tresor gespeichert, aus welchem sie später dynamisch geladen und ausgeführt werden können und die empfangene Datei sowie sämtliche temporären Dateien werden an Block 1512 entfernt. Nach dem Import eines kryptographischen Provider-Pakets und dem Extrahieren der kryptographischen Provider-Implementierung für die Plattform, auf welcher eine kryptographische Suite-Management-Einheit gehostet wird, kann die kryptographische Suite-Management-Einheit die Elemente des Pakets verwerfen, die für die Host-Plattform ungeeignet sind, um Platz zu schaffen. Zum Beispiel kann die kryptographische Suite-Management-Einheit während des Imports eines kryptographischen Provider-Pakets das Paket in dem Speicher speichern, die relevanten verteilbaren Information extrahieren und in dem Suite-Tresor speichern und die irrelevanten verteilbaren Informationen, wie aus Fig. 15 ersichtlich, verwerfen. Alternativ können die verteilbaren Informationen für alle Plattformen, falls zutreffend, in dem Suite-Tresor gespeichert werden. Wenn die empfangende Anwendung den kryptographischen Provider zum Beispiel für noch eine andere Anwendung importieren muss und die dem importier-

ten kryptographischen Provider-Paket zugeordnete Richtlinie dies erlaubt, kann sich die empfangende kryptographische Suite-Management-Einheit dafür entscheiden, alle verteilbaren Informationen in dem Suite-Tresor zu speichern. In weiteren Aspekten ermöglicht es die kryptographische Suite-Management-Einheit einem Akteur, der eine bestimmte kryptographische Provider-Implementierung besitzt, einem vertrauenswürdigen Partner die Verwendung der Implementierung zu erlauben, entweder mit oder ohne Einschränkungen wie zum Beispiel Parametern hinsichtlich der Zeit und/oder der Verwendung und/oder der Speicherung. Daher kann eine Plattform einen Lizenzmanager umfassen oder mit einem solchen kommunizieren, der konfiguriert ist, um eine Lizenzdatei zu generieren, die potenzielle Einschränkungen umfasst und dem vertrauenswürdigen Partner bereitgestellt werden soll.

[0069] Die Import-/Exportoperationen können als ein Protokoll strukturiert sein. Vorzugsweise beeinflusst die Ausführung des Protokolls nicht die Sicherheitsniveaus der «Besitzeranwendung» 1604 und der «Partneranwendung» 1602. Hier bezieht sich «Besitzeranwendung» auf eine Anwendung, die auf dem Gerät wie ein Akteur ausgeführt wird, der ein gegebenes Krypto-Paket besitzt, während sich «Partneranwendung» auf eine Anwendung bezieht, die einem vertrauenswürdigen Partner entspricht, der das Krypto-Paket, möglicherweise unter Lizenz, empfangen soll. Während dieses Protokolls trifft die kryptographische Suite-Management-Einheit Bestimmungen auf Grundlage der Werte des Sicherheitsniveaus der Anwendungen, in welche sie integriert wird, sowie der von den Anwendungen durchgesetzten Richtlinien wie die Lizenzierung. Das Protokoll kann ein Verschlüsselungsverfahren mit Public Key verwenden, wie in Fig. 16 als Verfahren 1600 veranschaulicht.

[0070] Wann immer eine Anwendung die Dienste eines spezifischen kryptographischen Provider-Pakets von der API der kryptographischen Suite-Management-Einheit, wie an Block 1606 veranschaulicht, anfordert, kann die kryptographische Suite-Management-Einheit an Block 1608 überprüfen, ob die Nutzungsbedingungen noch gültig sind. Falls die Lizenzbedingungen anzeigen, dass der kryptographische Provider nicht länger für diese Anwendung und/oder das Gerät zugelassen ist, kann die kryptographische Suite-Management-Einheit automatisch (d. h. ohne weitere Benutzereingaben) das angeforderte kryptographische Provider-Paket aus dem Suite-Tresor löschen. Falls die Lizenz jedoch weiterhin gültig bleibt, kann die kryptographische Suite-Management-Einheit das Provider-Paket entschlüsseln und dynamisch die gemeinsamen Bibliotheken, wie zuvor beschrieben, laden, wie an den Blöcken 1616, 1618 veranschaulicht. Das in Bezug auf Fig. 16 beschriebene Verfahren kann einen gemeinsamen kryptographischen Provider, der zwischen der Besitzeranwendung, wie an den Blöcken 1610, 1612 veranschaulicht, dem Lizenzmanager und der Partneranwendung geteilt wird, für die Verschlüsselung und Entschlüsselung der dazwischen ausgetauschten Datei, erforderlich machen. Ein Verschlüsselungsverfahren mit Public Key wie zum Beispiel das ECIES (Elliptic Curve Integrated Encryption Scheme) verwendet werden.

[0071] Es wird gewürdigt, dass der kryptographische Besitzer möglicherweise nicht nur die Nutzungsbedingungen sondern auch die Umgebung, in welcher exportierte kryptographische Provider-Pakete verwendet werden, steuern möchte. Daher kann die Lizenzdatei, die das kryptographische Provider-Paket begleitet, das an den vertrauenswürdigen Partner gesendet wird, eine oder mehrere Einschränkungen wie zum Beispiel die folgenden Parameter umfassen:

- Anfangsdaten und die Dauer, für die das Paket von der vertrauenswürdigen Anwendung verwendet werden kann;
- die Gesamtmenge an Daten (z. B. Anzahl von Bytes), die unter Verwendung des kryptographischen Provider-Pakets verschlüsselt oder entschlüsselt werden können;
- eine minimale oder maximale Schlüsselgrösse, die mit dem kryptographischen Provider-Paket verwendet werden kann (die kryptographische Suite-Management-Einheit kann es zusammen mit der Partneranwendung, nachdem dieser Parameter auftritt, verbieten, dass nicht konforme Schlüsselgrössen mit dem kryptographischen Provider verwendet werden, auch wenn die darin enthaltenen Algorithmen dies unterstützen);
- eine minimale Schlüsselgrösse des Krypto-Providers der von dem Suite-Tresor der kryptographischen Suite-Management-Einheit verwendet wird, der in Verbindung mit der Partneranwendung ausgeführt wird (dies kann verwendet werden, um ein unsicheres Speichern des kryptographischen Providers durch die Partneranwendung zu vermeiden); und
- eine Markierung, die anzeigt, ob die Partneranwendung Zugriff auf einen Hardware-Schlüsseltresor haben muss oder ob ein Software-Schlüsseltresor ausreichend ist.

[0072] In Aspekten wird ein sicherer Schlüsseltresor bereitgestellt, um Schlüssel für die Verschlüsselung sicher zu speichern, was in Form eines sicheren Software-Schlüsseltresors oder eines sicheren Hardware-Schlüsseltresors erreicht werden kann.

[0073] Während der Ausführung einer kryptographischen Funktion, kann die kryptographische Suite-Management-Einheit aufgerufen werden, um ein asymmetrisches Schlüsselpaar zu generieren und den Private Key zu speichern. Es ist jedoch möglich, dass die Host-Plattform für die kryptographische Suite-Management-Einheit keine grundsätzlich sicheren Speichermöglichkeiten umfasst. Sofern die Host-Plattform nicht ein zugehöriges sicheres Modul für die Ausführung kryptographischer Provider-Implementierungen umfasst, können die in dem kryptographischen Provider-Paket enthaltenen Algorithmen in das System der Host-Plattform geladen werden, um kryptographische Operationen auszuführen. Falls

der Systemspeicher gefährdet ist, können schädliche Elemente auf die Algorithmen zugreifen. Ferner können Elemente der kryptographischen Provider-Implementierung, die in dem dauerhaften Speicher gespeichert sind, ebenso durch eine innewohnende Unsicherheit der Host-Plattform enthüllt werden.

[0074] Nun wird in Bezug auf Fig. 17 ein Verfahren 1700 zum Bereitstellen eines sicheren Software-Schlüsseltresors in der kryptographischen Suite-Management-Einheit 112 veranschaulicht. Der Schlüsseltresor 136 speichert Schlüssel in verschlüsselter Form im dauerhaften Speicher wie einem Dateisystem 106 auf dem Zielgerät, sodass sie nicht von unbefugten Benutzern oder Anwendungen entschlüsselt werden können. In Ausführungsformen generiert und verwendet der Schlüsseltresor für jedes Gerät einen eindeutigen Geräteschlüssel für Schlüssel zum Verschlüsseln und Entschlüsseln in dem Schlüssel-Tresor, wie an den Blöcken 1702, 1704, 1706 gezeigt. Die Preisgabe des Geräteschlüssels gegenüber einem unbefugten Benutzer bzw. einer Anwendung würde ebenso zu einer Preisgabe aller in dem Schlüsseltresor gespeicherten Schlüssel führen und daher müssen Mechanismen implementiert werden, um die Geheimhaltung des Geräteschlüssels zu schützen.

[0075] Nun wird in Bezug auf Fig. 18 in Ausführungsformen ein White Box-Verschlüsselungsverfahren gezeigt, wobei die Schlüssel und Algorithmen für die White Box-Verschlüsselung während der Aufbauzeit der Anwendung entstellt werden. Sobald die Anwendung entwickelt wurde, können geeignete Aufbau-Tools aufgerufen werden, um den Quellcode in Binärdateien umzuwandeln, die mit der Zielplattform kompatibel sind. Um ein White Box-Modul 1802 bereitzustellen können ein Schlüssel (oder ein Schlüsselpaar) und die binären Objekte für die kryptographische Suite-Management-Einheit (welche das White Box-Modul umfassen) durch White Box-Tools geleitet werden, um die Schlüssel und den White Box-Modulcode zu entstellen. Die resultierenden Binärdateien können dann an ein standardmässiges Verknüpfungsmittel weitergegeben werden, um die finale Binärdatei für die Anwendung zu erzeugen, welche in sich Code für die kryptographische Suite-Management-Einheit enthält, der das White Box-Modul umfasst. Es wird gewürdigt, dass jeder Akteur, der Anwendungen aufbaut, welche die kryptographische Suite-Management-Einheit zusammen mit dem White Box-Modul umfassen, die in dem White Box-Modul enthaltenen kryptographischen Algorithmen umfasst. Um die Veröffentlichung solcher Algorithmen zu verhindern, kann das White Box-Modul von einer vertrauenswürdigen Partei in entstelltem Binärformat an Anwendungsbauer versandt werden, sodass nur die vertrauenswürdige Partei die kryptographischen Algorithmen in dem White Box-Modul besitzt. Alternativ können die Schlüsselgenerierung und Entstellung als ein Cloud- oder Internet-basierter Dienst von einer vertrauenswürdigen Partei ausgeführt werden.

[0076] Das resultierende White Box-Modul enthält einen entstellten Schlüssel, der verwendet werden kann, um einen Geräteschlüssel für die Host-Plattform zu entschlüsseln. Bei der Laufzeit auf dem Gerät eines Endnutzers kann eine Anwendung 102, die eine kryptographische Suite-Management-Einheit 112 verwendet, die das resultierende White Box-Modul umfasst, einen der Private Keys entschlüsseln, der in dem Schlüsseltresor gespeichert ist, indem, gemäss einem in Fig. 18 gezeigten Verfahren 1800, ein Aufruf an die kryptographische Suite-Management getätigt, wird, wie an Block 1802 gezeigt, um: den Geräteschlüssel wiederherzustellen; ihn zu entschlüsseln, ohne ihn in dem Systemspeicher an Block 1804 preiszugeben; den Geräteschlüssel zu verwenden, um den Private Key an den Blöcken 1806, 1808 zu entschlüsseln; und den Private Key in entschlüsselter Form an die aufrufende Komponente, wie gezeigt, zurückzuschicken. Vorzugsweise, sobald das White Box-Modul den angeforderten Private Key entschlüsselt hat, leert es umgehend und sicher den Speicher, der den entschlüsselten Geräteschlüssel enthält, wie an Block 1810 gezeigt. Der angeforderte Private Key kann dann an die aufrufende kryptographische Suite-Management-Einheit-Komponente zurückgeschickt werden.

[0077] Noch vorzugsweiser kann das White Box-Modul sicherstellen, dass Puffer, die zum temporären Speichern des entschlüsselten Private Keys, bevor dieser an den Aufrufer zurückgeschickt wird, verwendet werden, sicher gelöscht werden, sodass der Geräteschlüssel und der angeforderte Private Key nach dem Zurückschicken an den Aufrufer nicht mehr in dem Speicher liegen.

[0078] In weiteren Ausführungsformen kann der Schlüsseltresor eine Passwort-basierte Herangehensweise verwenden, wobei die Geheimhaltung des Geräteschlüssels durch das Verschlüsseln des Geräteschlüssels unter Verwendung eines kryptographischen Providers gewährleistet wird, der für die kryptographische Suite-Management-Einheit verfügbar ist, die einen Schlüssel verwendet, der von einem Passwort abgeleitet wird, das von dem Benutzer des Geräts bereitgestellt wird. Eine Anwendung, die auf dem Gerät ausgeführt wird, welches die kryptographische Suite-Management-Einheit verwendet, würde den Benutzer in Bezug auf das Passwort des Geräteschlüssels unter Verwendung der Anwendungsbenutzerschnittstelle auffordern und das Passwort mittels eines API-Aufrufs an die kryptographische Suite-Management-Einheit liefern. Unter Verwendung des von dem Benutzer bereitgestellten Passworts kann der Schlüsseltresor den verschlüsselten Geräteschlüssel aus dem dauerhaften Speicher laden, den Schlüssel für die Entschlüsselung ableiten, der benötigt wird, um den Geräteschlüssel zu entschlüsseln und den Geräteschlüssel verwenden, um beliebige der Schlüssel zu entschlüsseln, die sicher durch den Schlüsseltresor gespeichert sind. Wie bei dem Verfahren, bei welchem ein White Box-Verschlüsselungsverfahren eingesetzt wird, wird auch bei diesem Verfahren sichergestellt, dass das von dem Benutzer bereitgestellte Passwort und der verschlüsselte Geräteschlüssel nicht länger in einem unverschlüsselten oder nicht entstellten Format in dem flüchtigen Speicher gespeichert werden, als für die Ausführung der Funktionen des Schlüsseltresors erforderlich und dass die dazu verwendeten Puffer sicher gelöscht werden. Zudem wird der Schlüsseltresor das von dem Benutzer bereitgestellte Passwort oder den entschlüsselten Geräteschlüssel niemals im dauerhaften Speicher ablegen.

[0079] Als Alternative zu einer Softwareimplementierung des sicheren Schlüsselcontainers kann die kryptographische Suite-Management-Einheit ein sicheres Schlüsseltresormodul umfassen, das eine Hardware-basierte manipulationssiche-

re Plattform wie ein Hardware Secure Module (HSM) oder ein sicheres Element (SE) verwendet, das auf der Hardware-Plattform des Geräts, welches die kryptographische Suite-Management-Einheit hostet, gehostet wird. Da das HSM oder SE von anderen Anwendungen verwendet werden kann, kann die kryptographische Suite-Management-Einheit lediglich den Geräteschlüssel speichern - im Gegensatz zu anderen Private Keys, die benötigt werden, um andere Schlüssel oder sensible Daten, die in dem Schlüsseltresor gespeichert sind, freizuschalten. Durch die Verwendung des SEs wird der Geräteschlüssel gegenüber dem Systemspeicher nicht preisgegeben.

[0080] Eine Schwachstelle bei der Verwendung des Hardware-SEs ist, dass beliebige Private Keys, die zur Entschlüsselung von Paketdateien des kryptographischen Providers benötigt werden, für die Dauer einer zugehörigen Entschlüsselungsoperation in dem Speicher liegen können. Das kryptographische Provider-Paket kann jedoch gegenüber Offline-Attacken geschützt sein, an der Stelle, wo der dauerhafte Speicher, der die verschlüsselten Paketdateien des Providers und die Private Keys in dem Schlüsseltresor enthält, aufgrund der Tatsache, dass sich der Geräteschlüssel, der zum Entschlüsseln aller Informationen benötigt wird, sicher innerhalb des sicheren Elements befindet.

[0081] Zusätzlich zu dem Schlüsseltresor kann die kryptographische Suite-Management-Einheit zusammen mit einem Suite-Tresor für die Implementierung, den Import und das sichere Speichern verschlüsselter kryptographischer Provider-Pakete operieren. Wie der oben beschriebene Schlüsseltresor kann der Suite-Tresor als eine Hardware- oder Softwarelösung implementiert werden. Nun wird in Bezug auf Fig. 19 eine illustrative Durchführung eines Verfahrens 1900 zum Zugriff auf sicher gespeicherten Code aus einem mit Software implementierten Suite-Tresor veranschaulicht. Bei der illustrativen Durchführung wird das kryptographische Provider-Paket, bevor es in dem dauerhaften Speicher des Suite-Tresor-Moduls (an Element 1903) gespeichert wird, unter Verwendung eines lokalen, gerätespezifischen Schlüssels für die Verschlüsselung, wie an Block 1902 gezeigt, verschlüsselt. Wenn die kryptographische Suite-Management-Einheit bestimmt, dass ein Zugriff auf das kryptographische Provider-Paket notwendig ist, ruft es den Suite-Tresor zum Laden des Pakets auf, wie als Element 1904 veranschaulicht. Nach dem Empfang des Aufrufs liest der Suite-Tresor das verschlüsselte kryptographische Paket aus dem Dateisystem der Hostplattform, wie an Element 1905, 1906 veranschaulicht; an Block 1908 entschlüsselt der Suite-Tresor das kryptographische Provider-Paket unter Verwendung des erhaltenen Private Keys und speichert die unverschlüsselten ausführbaren Informationen des kryptographischen Providers in einem sicheren Bereich wie einer virtuellen RAM-Disk oder einem vertrauenswürdigen Dateisystem wie einer Bibliothek, um sie für das OS zum dynamischen Laden verfügbar zu machen, wie an Element 1910 veranschaulicht. Der Suite-Tresor erstellt dann Aufrufe an das Betriebssystem des Hosts, um die unverschlüsselte Bibliothek in den Speicher zu laden, wie an Element 1912 veranschaulicht. Die unverschlüsselte Bibliothek liegt in dem Speicher, bis die Anwendung die Bibliothek nicht länger benötigt. Die Anwendung erstellt vorzugsweise einen Aufruf an die kryptographische Suite-Management-Einheit, wenn sie die Bibliothek nicht länger benötigt, sodass die kryptographische Suite-Management-Einheit den Suite-Tresor aufruft, um die unverschlüsselte Bibliothek aus dem Speicher zu entfernen.

[0082] Nun ruft die kryptographische Suite-Management-Einheit in Bezug auf Fig. 20 gemäss einem Verfahren 2000, nachdem sie aufgerufen wurde, um die unverschlüsselte Bibliothek aus dem Speicher zu entfernen, den Suite-Tresor auf, um die unverschlüsselte Bibliothek sicher aus dem Arbeitsspeicher und von der Festplatte zu löschen, wie an Element 2002 veranschaulicht. Wenn zum Beispiel eine virtuelle RAM-Disk verwendet wird, kann die Bibliothek unter Verwendung eines 3-Pass-Wipes überschrieben werden.

[0083] Alternativ kann die kryptographische Suite-Management-Einheit für die Verwendung mit einem Suite-Tresor als eine Hardware-Implementierung zum Beispiel unter Verwendung eines Hardware Security Module (HSM) konfiguriert sein, sofern das Hostgerät ein solches HSM umfasst. Wenn ein HSM verwendet wird, um das kryptographische Provider-Paket zu hosten, können die in dem HSM enthaltenen Funktionen während der Laufzeit nicht modifiziert oder aktualisiert werden. Das bedeutet, dass das HSM dadurch eingeschränkt sein kann, dass es während der Laufzeit keine kryptographischen Provider-Pakete importieren kann, wie es in Bezug auf Software-Suite-Tresor-Implementierungen beschrieben wird.

[0084] Fig. 21 veranschaulicht eine exemplarische Konfiguration, bei welcher die kryptographische Suite-Management-Einheit 112 auf einer Plattform, die einen HSM-basierten Suite-Tresor umfasst, Verschlüsselungsoperationen aufruft. Das HSM 2102 kann eine Schnittstelle wie zum Beispiel einen PKCS11-Treiber 2104 umfassen. Wie gezeigt, kann das HSM eine PCIx-Karte 2106 sein, die in einer Linux-Umgebung installiert ist. Authentifizierungsinformationen für eine Anwendung, die Verschlüsselungsoperationen anfordert, können ausserhalb des HSM gespeichert werden, wie nachfolgend ausführlicher beschrieben.

[0085] Im Betrieb aktiviert die kryptographische Suite-Management-Einheit, wie in Fig. 21 und ausführlicher in Fig. 22 veranschaulicht, wenn eine Anwendung 102 die kryptographische Suite-Management-Einheit 112 aufruft, um eine Verschlüsselungsoperation aufzurufen, die von einem kryptographischen Provider-Paket definiert wird, das in dem HSM 2102 liegt, ihren HW-Client 2108 (veranschaulicht an Element 2202), um Client-Credentials 2110 (z. B. ein Client-Zertifikat) an Element 2204 zu erhalten, welche vorzugsweise von dem zuvor beschriebenen Schlüsseltresor an Element 2206 erhalten werden. Der HW-Client 2108, welcher konfiguriert ist, um mit dem PKCS11-Treiber 2104 des HSM 2102 zu kommunizieren, liefert die Credentials entschlüsselt für die Authentifizierung an Element 2208 an das HSM. Sobald das HSM 2102 die kryptographische Suite-Management-Einheit authentifiziert hat, ruft der HW-Client das HSM auf, um eine Verschlüsselungsoperation an Element 2210 durchzuführen und den HW-Client von dem HSM an Element 2212 abzumelden, wenn dies abgeschlossen ist. Der HW-Client schickt das Ergebnis der Verschlüsselungsoperation an die kryptographische Suite-Management-Einheit an dem veranschaulichten Element 2214 zur Lieferung an die aufrufende Anwendung zurück.

[0086] In dem in den Fig. 21 und 22 veranschaulichten Szenario liefert die kryptographische Suite-Management-Einheit zur Authentifizierung Client-Credentials an das HSM. Wie zuvor beschrieben, werden diese vorzugsweise von dem Schlüsseltresor 136 erhalten. Um die Client-Credentials anfänglich in dem Schlüsseltresor 136 zu platzieren, erhält sie die kryptographische Suite-Management-Einheit 112 von der aufrufenden Anwendung, wie in Fig. 23 veranschaulicht. Sobald die Anwendung oder der Endnutzer der Anwendung die Client-Credentials erhält, liefert die Anwendung die Credentials an den CM 132 der kryptographischen Suite-Management-Einheit 112, veranschaulicht an Element 2302, sowie den Pfad zu dem PKCS#11-Treiber. Die kryptographische Suite-Management-Einheit 112 speichert die Credentials in dem Schlüsseltresor, wie an Element 2304 veranschaulicht und aktualisiert den CM 132, um den Pfad zu dem PKCS#11-Treiber zu speichern.

[0087] In Aspekten kann es ein System für das kryptographische Suite-Management, wie zuvor beschrieben, einer Anwendung ermöglichen, eine Vielzahl kryptographischer Funktionen von einer Vielzahl kryptographischer Provider-Implementierungen aufzurufen. Die kryptographische Suite-Management-Einheit kann fermer eine API für die kryptographische Abstraktion zum Zugriff auf kryptographische Funktionen der verfügbaren kryptographischen Suites umfassen. Die API für die kryptographische Abstraktion kann abstrahierte kryptographische Primitive umfassen, die es Anwendungen ermöglichen, unterschiedliche kryptographische Provider-Implementierungen zu erstellen. Die API für die kryptographische Abstraktion kann als eine Reihe von APIs verstanden werden, von denen jede eine Gruppierung von Operationen darstellt, die von den zugrunde liegenden kryptographischen Provider-Implementierungen durchgeführt werden. Zum Beispiel kann die API für die kryptographische Abstraktion unter anderem die folgende Reihe von APIs umfassen:

- Zufallszahl-API;
- Hash-Funktion-API;
- Public-Key-Chiffre-API; und
- API für symmetrische Verschlüsselungen.

[0088] Ferner kann die API für die kryptographische Abstraktion Folgendes umfassen: Funktionen, die es einer aufrufenden Anwendung ermöglichen, den Bereich der Werte zu bestimmen, die für die spezifische aufgerufene kryptographische Provider-Implementierung geeignet sind; und Fehler- und Return-Statuscodes, die für verschiedene kryptographische Provider-Implementierungen zum Kommunizieren des Status an die aufrufende Anwendung üblich sind. Zum Beispiel kann die API für die kryptographische Abstraktion in Bezug auf Fig. 24 in ihrer Reihe eine Blockchiffre-API 2402 umfassen. Die Blockchiffre-API kann wiederum die folgenden Primitive umfassen, um zugeordnete Funktionen aufzurufen:

- init_cipher: Funktion, die verwendet wird, um die Parameter der Blockchiffre-Implementierung zu initialisieren;
- generate_key: Funktion, die verwendet wird, um den Schlüsselplan für die Verschlüsselung und/oder Entschlüsselung festzulegen;
- encrypt: Funktion, die verwendet wird, um einen Datenblock zu verschlüsseln; und
- decrypt: Funktion, die verwendet wird, um einen Datenblock zu entschlüsseln.

[0089] Es wird mit demselben Beispiel fortgefahren, wobei die init_cipher-Funktion eine Liste von Argumenten erfordern kann, die für Blockchiffre-Implementierungen geeignet sind wie:

- Schlüsselgrösse;
- Schlüsselwert;
- Blockgrösse; und
- Chiffre-Modus.

[0090] In verschiedenen kryptographischen Provider-Implementierungen können jedoch einige Implementierungen verschiedene Wertebereiche für die Argumente zulassen. Zum Beispiel kann Krypto-Provider-A nur Schlüsselgrössen von 128 und 256 Bit unterstützen, während Krypto-Provider-B Schlüsselgrössen von 128, 256, 512 und 1024 Bit unterstützen kann. Daher kann die Blockchiffre-API 2402 die folgenden Primitive umfassen, um für eine gegebene kryptographische Provider-Implementierung zulässige Wertebereiche an die aufrufende Anwendung zurückzuschicken:

- get_key_sizes
- get_block_size_range

- get_cipher_modes

[0091] Wie aus Fig. 24 ersichtlich kann die aufrufende Anwendung 102 gemäss einem Verfahren 2400 zunächst einen Aufruf an die kryptographische Suite-Management-Einheit 112 initialisieren, um zum Beispiel zulässige Schlüsselgrössen, Bereiche für Blockgrössen und Chiffre-Modi für eine kryptographische Provider-Implementierung zurückzuschicken. Die aufrufende Anwendung kann dann die zurückgeschickten Parameter verwenden, um zulässig Aufrufe gemäss den verfügbaren Primitiven zu initialisieren. Der folgende Pseudocode ist illustrativ für das in Fig. 24 gezeigte Szenario:

```
int     keySizeArray[]; int     numKeyEntries;
int     minBlockSize,maxBlockSize; int     cipherModes[];
int     numCipherModes;
/* error checking omitted for readability */
get_key_sizes(keySizeArray, &numKeyEntries);
get_block_size_range(&minBlockSize,&maxBlockSize);
get_cipher_modes(cipherModes, numCipherModes);
/*initialize the cryptographic provider with the largest key size, smallest block size
and first available block mode
*/
init_cipher(key_sizes[numKeyEntries-1], minBlockSize, cipherModes[0], ...);
encrypt(data);
```

[0092] In weiteren Aspekten kann ein System für das kryptographische Suite-Management Dienste für die Überschreibung zwischen Parteien ermöglichen, die verschiedene kryptographische Algorithmen aufrufen. In bestimmten Szenarien können zwei Parteien, die sicher miteinander kommunizieren möchten, verschiedene kryptographische Provider-Implementierungen für die Verschlüsselung und Entschlüsselung verwenden. Für den Fall, dass jede Partei die kryptographische Provider-Implementierung mit der anderen nicht teilen möchte oder dazu nicht in der Lage ist, kann ein zwischengeschaltetes Gateway in Bezug auf die Daten als Vertretung agieren und die Daten umwandeln, sodass sie unter Verwendung der kryptographischen Provider-Implementierung, die bei der empfangenden Anwendung verfügbar ist, entschlüsselt werden können, was als ein Dienst für die Überschreibung bezeichnet wird. Das Gateway kann zum Beispiel ein VoIP-Call-Server sein, der eine Austauschsequenz einer SIP-Nachricht verwendet, um eine VoIP-Verbindung zwischen den zwei Parteien herzustellen. In dem vorhergehenden Beispiel kann die erste Partei eine SIP-INVITE-Nachricht verschicken, welche die SIP-URL der empfangenden Partei umfasst. Alternativ kann das Gateway ein HTTP-Proxy-Server sein, bei dem sich eine erste Partei sicher mit dem HTTP-Proxy-Server verbindet und die URL des HTTP-Servers (d. h. die zweite Partei) bereitstellt, mit welchem sie verbunden werden möchte. Der Dienst für die Überschreibung wird von einem Überschreibungsmodul bereitgestellt, welches auf einer kryptographischen Suite basiert.

[0093] Fig. 25 veranschaulicht eine Gatewaykonfiguration 2500 zum Bereitstellen von Proxy- und Überschreibungsdiensten. Das Gateway umfasst: eine Gatewaylogik 2502, welche konfiguriert ist, um Aufrufe an ein Überschreibungsmodul über eine Transcript-API 2504 zu tätigen. Das Überschreibungsmodul umfasst einen Verbindungsplan für die Überschreibung 2506 zur Abbildung der Kommunikationsparameter für jeden Endpunkt (d. h. Partei). Das Überschreibungsmodul ist konfiguriert, um kryptographische Provider-Implementierungen über eine kryptographische API 2508 aufzurufen, welche die kryptographischen Provider-Implementierungen umfassen, die von beiden Parteien verwendet werden.

[0094] Fig. 26 veranschaulicht ein Verfahren 2600 zum Bereitstellen von Proxy- und Überschreibungsdiensten unter Verwendung des Gateways. Das Gateway 2602 stellt eine Verbindung zwischen zwei Endpunkten her. Das Gateway identifiziert dann die Verbindung zwischen den zwei Endpunkten (d. h. Parteien) (2604, 2606), indem er den beiden Parteien Statusinformationen zuordnet; und das Gateway verwendet die Statusinformationen, um die Kommunikationsparameter festzulegen, die jedem Endpunkt zugeordnet werden, veranschaulicht an Block 2608. Die Kommunikationsparameter für jeden Endpunkt umfassen:

- Die IP-Adresse und das Protokoll (TCP oder UDP) des Endpunkts;

- Den TCP- oder UDP-Port der Verbindung;
- Das kryptographische Provider-Paket, das verwendet wird, um die mit diesem Endpunkt ausgetauschten Daten zu verschlüsseln und/oder entschlüsseln; und
- Die Sitzungsschlüssel zum Verschlüsseln und/oder Entschlüsseln von Daten, die mit diesem Endpunkt ausgetauscht werden.

[0095] Sobald das Gateway die Kommunikationsparameter für jeden Endpunkt erhält, erstellt es über die Überschreibungs-API einen Aufruf an das Überschreibungsmodul, um ein Planverfahren, veranschaulicht als Element 2610, aufzurufen. Das Planverfahren speichert die Kommunikationsparameter in dem Verbindungsplan für die Überschreibung. Jedem Eintrag in dem Verbindungsplan für die Überschreibung wird eine eindeutige Verbindungs-ID zugewiesen.

[0096] Wenn ein erster Client verschlüsselte Daten an das Überschreibungs-Gateway, wie an Element 2612 veranschaulicht, überträgt, ruft das Gateway 2603 das Überschreibungsmodul über die Überschreibungs-API 2605, wie an Element 2614 beschrieben, auf, welches die folgenden Parameter bereitstellt:

- Die eindeutige Verbindungs-ID, die durch den früheren Aufruf an das Planverfahren zurückgeschickt wurde;
- Die verschlüsselten Daten, die von dem ersten Client-Endpunkt empfangen wurden; und
- Eine Absenderkennung (z. B. IP-Adresse), welche den ersten Client-Endpunkt identifiziert.

[0097] Das Überschreibungsmodul führt dann an Block 2616 die folgenden Operationen aus: (i) es verwendet die Verbindungs-ID, um in dem Verbindungsplan für die Überschreibung den Eintrag zu lokalisieren, der zu der Verbindungs-ID gehört; (ii) es ruft die kryptographische Provider-Implementierung auf, die zu der Verbindungs-ID für den ersten Client-Endpunkt gehört, um die Daten zu entschlüsseln; (iii) es ruft die kryptographische Provider-Implementierung auf, die zu der Verbindungs-ID für den zweiten Client-Endpunkt gehört, um die entschlüsselten Daten zu verschlüsseln; und (iv) es schickt die erneut verschlüsselten Daten als ein Puffer zurück an den Aufrufer, an Element 2618. Das Gateway überträgt dann den erneut verschlüsselten Puffer an den zweiten Client, wie an Element 2620 veranschaulicht.

[0098] Wenn Daten überschrieben werden müssen, liefert die Anwendung die Verbindungs-ID des Absenders, die Verbindungs-ID des Ziels und die verschlüsselten Daten an den Überschreibungsdienst, der in der sicheren Computerumgebung ausgeführt wird und erhält die überschriebenen Daten von dem Dienst zurück. Das kryptographische Suite-Management gibt die Interna des Überschreibungsdienstes gegenüber der Anwendung nicht preis.

[0099] In Aspekten können die kryptographischen Provider-Pakete, die damit verknüpften Richtlinien und die Sammlung kryptographischer Suite-Management-Einheiten, die alle Teil einer gegebenen administrativen Domäne sind, von einem Policy Manager, wie in Fig. 27 veranschaulicht, verwaltet werden. In Ausführungsformen kann der Policy Manager 2700 aus Folgendem bestehen: einer Anwendungsbenutzerschnittstelle 2702 für die Interaktion mit Anwendungsbenutzern; einer Komponente für die Policy Management Logik 2704, welche die Funktionen bereitstellt, die benötigt werden, um die Sammlung kryptographischer Provider-Pakete 2706, der Richtlinien 2708 und Endpunkte 2710 zu verwalten und mit den kryptographischen Suite-Management-Einheiten 2712 in der administrativen Domäne kommuniziert; eine Krypto-Provider-DB, welche die Sammlung aller kryptographischen Provider-Pakete enthält, die in der administrativen Domäne verfügbar sind, eine Richtlinien-DB, welche die Sammlung der Richtlinien enthält, die für jedes kryptographische Provider-Paket angewendet werden können und eine Endpunkt-DB, welche Informationen über jede kryptographische Suite-Management-Einheit in der administrativen Domäne enthält, umfassend Informationen, die für eine sichere Kommunikation mit dem Endpunkt benötigt werden (z. B. IP-Adresse und Sicherheits-Credentials).

[0100] In Ausführungsformen kann der Policy Manager mit einer oder mehreren kryptographischen Suite-Management-Einheiten über ein Netzwerk 2714 kommunizieren, um kryptographische Provider-Pakete zu verteilen; um kryptographische Provider-Pakete, die in einer kryptographischen Suite-Management-Einheit verfügbar sind, zu löschen; um Informationen über Richtlinien, die mit einem oder mehreren kryptographischen Provider-Paketen verknüpft sind, zu kommunizieren; um Konfigurationsinformationen für die kryptographische Suite-Management-Einheit zu kommunizieren; um von einer kryptographischen Suite-Management-Einheit Statistiken im Hinblick auf Status und Leistung zu erhalten; und/oder um für eine kryptographische Suite-Management-Einheit ein Management- oder Sicherheitsaudit durchzuführen. Es sollte beachtet werden, dass der Policy Manager eine optionale Komponente der Lösung ist. Administrative Benutzer können die gleichen Operationen mit individuellen Instanzen von kryptographischen Suite-Management-Einheiten durch die verfügbaren Anwendungsbenutzerschnittstellen und die APIs der kryptographischen Suite-Management-Einheiten ausführen. Zudem können sämtliche Operationen, die an dem Export/Import kryptographischer Provider-Pakete zwischen Instanzen von kryptographischen Suite-Management-Einheiten und der zugehörigen Funktionalität zum Definieren und Durchsetzen von Nutzungsrichtlinien und zugehörigen Sicherheitsmassnahmen beteiligt sind, ohne die Verwendung der Policy Manager-Komponente, wie zuvor in den zugehörigen Abschnitten beschrieben, erreicht werden.

[0101] Die Sammlung von Instanzen für kryptographische Suite-Management-Einheiten, welche wie in der Endpunkt-DB nachvollzogen verwaltet werden, kann durch eine Vielzahl von Methoden befüllt werden, die Folgendes umfassen: manuell durch einen administrativen Benutzer bereitgestellt; automatisch mittels eines Discovery-Protokolls bereitgestellt, wobei die Komponente der Policy Management Logik das Netzwerk abtastet, um Instanzen kryptographischer Suite-Management-Einheiten zu finden oder mittels eines Registrierungsprotokolls, wobei Instanzen von kryptographischen Suite-Management-Einheiten mit einem bestimmten Policy Manager registriert werden. Die Policy Management Logik stellt die Funktionalität bereit, die benötigt wird, um entweder als Reaktion auf eine Benutzeraktion oder durch einen automatisierten Vorgang neue Einträge zu der Endpunkt-DB hinzuzufügen, existierende zu aktualisieren oder Einträge aus der Endpunkt-DB zu löschen.

[0102] Obwohl die Erfindung in Bezug auf bestimmte spezifische Ausführungsformen beschrieben wurde, sind für einen Fachmann verschiedene diesbezügliche Modifikationen offenkundig. Der Umfang der Patentansprüche sollte nicht durch die bevorzugten Ausführungsformen beschränkt werden, sondern sollte die umfassendste Auslegung aufweisen, die mit der Beschreibung als Ganzes vereinbar ist. Die gesamten Offenlegungen von allen zuvor genannten Referenzen werden hierin durch Bezugnahme eingefügt.

Patentansprüche

1. Es wird Folgendes beansprucht:
   1. Verfahren für kryptographisches Suite-Management, umfassend

   a. Konfigurieren eines ersten Korrespondenten, der mit einer ersten kryptographischen Suite-Management-Einheit verbunden ist, um eine Importanfrage an einen zweiten Korrespondenten zu übertragen, der mit einer zweiten kryptographischen Suite-Management-Einheit verbunden ist, wobei die Anfrage die Identifizierung einer kryptographischen Implementierung und Sicherheitsanforderungen für die kryptographische Implementierung für den Export durch den zweiten Korrespondenten umfasst;

   b. Konfigurieren einer zweiten kryptographischen Suite-Management-Einheit, um die kryptographische Implementierung bereitzustellen, die unter Verwendung der Sicherheitsanforderungen konfiguriert wird;

   c. Konfigurieren des zweiten Korrespondenten, um die konfigurierte kryptographische Implementierung zu dem ersten Korrespondenten zu exportieren; und

   d. Konfigurieren der ersten kryptographischen Suite-Management-Einheit, um die konfigurierte kryptographische Implementierung für die Verwendung durch den ersten Korrespondenten sicher zu importieren.

2. Verfahren nach Anspruch 1, ferner umfassend das Konfigurieren eines dritten Korrespondenten zum interagieren mit dem zweiten Korrespondenten auf identische Weise wie die Interaktion zwischen dem ersten Korrespondenten und dem zweiten Korrespondenten, wobei der zweite Korrespondent ein vertrauenswürdiger Drittmittler ist, der die sichere Kommunikation zwischen dem ersten Korrespondenten und dem dritten Korrespondenten erleichtert.
3. Verfahren nach Anspruch 1, wobei jede kryptographische Suite-Management-Einheit konfiguriert ist, um eine Vielzahl kryptographischer Implementierungen für die Verwendung in einem gesicherten Suite-Tresor zu speichern und sie zu anderen Korrespondenten zu exportieren.
4. Verfahren nach Anspruch 3, wobei jede kryptographische Suite-Management-Einheit konfiguriert ist, um jede der Vielzahl von kryptographischen Implementierungen aus ihrem Suite-Tresor zur Verwendung in einer sicheren Kommunikation dynamisch zu laden.
5. Verfahren nach Anspruch 3, wobei der Suite-Tresor jede kryptographische Implementierung während der Speicherung verschlüsselt und eine Kopie der für die Verschlüsselung verwendeten Schlüssel speichert.
6. Verfahren nach Anspruch 5, wobei der Suite-Tresor nach einer Anfrage zum Erhalt der kryptographischen Implementierung die verschlüsselte kryptographische Implementierung und die Schlüssel erhält, die kryptographische Implementierung unter Verwendung der Schlüssel entschlüsselt, die Schlüssel sicher löscht, die kryptographische Implementierung in einem flüchtigen Speicher auf eine virtuelle Disk schreibt, die kryptographische Implementierung für eine anfragende Anwendung verfügbar macht und die kryptographische Implementierung von der virtuellen Disk entfernt.
7. Verfahren nach Anspruch 1, wobei die Anfrage und der Export als ein Protokoll strukturiert sind, das kryptographische und Sicherheitsanforderungen von Importern und Exportern sicher verhandelt.
8. Verfahren nach Anspruch 7, wobei das Protokoll ein Public-Key-Verschlüsselungsverfahren verwendet und Folgendes umfasst:

   a.

der erste Korrespondent sendet eine Importanfrage, umfassend seinen Public Key, das Sicherheitsniveau seiner Anwendung und das für den kryptographischen Provider zu erwartende Sicherheitsniveau sowie die Plattform, an den zweiten Korrespondenten;

b. der zweite Korrespondent analysiert die Anfrage unter Berücksichtigung des Sicherheitsniveaus seiner Anwendung und seiner Richtlinie für das kryptographische Suite-Management, sucht durch seine kryptographischen Provider nach einer Übereinstimmung und entscheidet, ob der Export durchgeführt werden soll oder nicht;

c. nachdem sich der zweite Korrespondent für den Export entschieden hat, erzeugt der zweite Korrespondent ein Exportpaket, umfassend:

   i. seinen Public Key,

   ii. das Sicherheitsniveau seiner Anwendung;

   iii. Informationen über die kryptographische Implementierung und die Implementierung;

   iv. die kryptographische Implementierung, verschlüsselt mit dem Public Key des ersten Korrespondenten und, falls nötig, dem Private Key des zweiten Korrespondenten;

d. das Paket wird zu dem ersten Korrespondenten exportiert;

e. der erste Korrespondent empfängt das Paket, extrahiert die Informationen und entscheidet - auf Grundlage der Informationen und seiner Managementrichtlinie -, ob er annehmen soll oder nicht;

f. der erste Korrespondent entschlüsselt die kryptographische Implementierung mit dem Private Key des zweien Korrespondenten und, falls nötig, dem Public Key des zweiten Korrespondenten.

9. Verfahren nach Anspruch 8, wobei das Public-Key-Verschlüsselungsverfahren ECIES (Elliptic Curve Integrated Encryption Scheme) ist.

10. Verfahren nach Anspruch 9, umfassend eine Registrierungsphase, wenn die ersten und zweiten Komponenten Endpunkte sind, wobei jeder Endpunkt seine kryptographische Implementierung zu der kryptographischen Suite-Management-Einheit exportiert, welche ein Vermittler in dem Kommunikationskanal zwischen den beiden Endpunkten ist, gefolgt von der Ausführung eines Schlüsselzustimmungsprotokolls zur Generierung symmetrischer Schlüssel für jedes der zwei Paare, umfassend die kryptographische Suite-Management-Einheit und jeden der Endpunkte.

11. Verfahren nach Anspruch 10, umfassend den Dienst der Übersetzung von Chiffretexten, die von einem ersten Endpunkt erzeugt wurden, in Chiffretexte des anderen zweiten Endpunkts.

12. Verfahren nach Anspruch 11, wobei der Übersetzungsdienst Folgendes umfasst:

a. den ersten Endpunkt, der einen Klartext mit seinem symmetrischen Verschlüsselungsverfahren und dem Schlüssel, der zwischen dem ersten Endpunkt und der kryptographischen Suite-Management-Einheit während der Registrierung eingeführt wurde, verschlüsselt;

b. Übertragen des resultierenden Chiffretexts an die kryptographische Suite-Management-Einheit;

c. die kryptographische Suite-Management-Einheit, die den resultierenden Chiffretext mit dem Verschlüsselungs-/Entschlüsselungsverfahren des ersten Endpunkts und dem während der Registrierung eingeführten Schlüssel entschlüsselt, den resultierenden Klartext mit dem Verschlüsselungssystem des zweiten Endpunkts und dem zwischen dem zweiten Endpunkt und der kryptographischen Suite-Management-Einheit während der Registrierung eingeführten Schlüssel verschlüsselt und den resultierenden Chiffretext an den zweiten Endpunkt sendet;

d. den zweiten Endpunkt, der den empfangenen Chiffretext mit seinem Entschlüsselungsverfahren und dem Schlüssel, der zwischen dem zweiten Endpunkt und der kryptographischen Suite-Management-Einheit während der Registrierung eingeführt wurde, entschlüsselt.

13. Verfahren nach Anspruch 1, wobei die kryptographische Suite-Management-Einheit ein dynamisches Linken kryptographischer Implementierungen für Anwendungen, die an den Korrespondenten ausgeführt werden, bereitstellt.

14. Verfahren nach Anspruch 1, wobei die kryptographische Suite-Management-Einheit die Integrität der kryptographischen Implementierungen sicherstellt, die für anfragende Anwendungen verfügbar gemacht werden.

15. Verfahren nach Anspruch 1, wobei die zweite kryptographische Suite-Management-Einheit konfiguriert ist, um Richtlinien festzulegen, die Nutzungsbedingungen der kryptographischen Implementierung bestimmen.

16. Verfahren nach Anspruch 15, wobei die Richtlinien Lizenzbedingungen umfassen, die Anwendungen und Geräte festlegen, denen eine Verwendung der kryptographischen Implementierung erlaubt ist.

17. Verfahren nach Anspruch 15, wobei die Richtlinien Lizenzbedingungen umfassen, die den Zeitrahmen festlegen, in dem die kryptographische Implementierung genutzt werden darf.
18. Verfahren nach Anspruch 15, wobei nach dem Versuch einer Anwendung oder eines Geräts, eine kryptographische Implementierung auf unerlaubte Weise zu verwenden, die kryptographische Suite-Management-Einheit die kryptographische Implementierung aus dem Suite-Tresor löscht.
19. Verfahren nach Anspruch 1, wobei der erste Korrespondent seinen Public Key in der Anfrage bereitstellt.
20. System für das kryptographische Suite-Management, umfassend einen zweiten Korrespondenten, der mit einer zweiten kryptographischen Suite-Management-Einheit verbunden ist, die konfiguriert ist, um mit einem ersten Korrespondenten zu kommunizieren, der mit einer ersten kryptographischen Suite-Management-Einheit verbunden ist, wobei nach Übertragung einer Importanfrage durch den ersten Korrespondenten an den zweiten Korrespondenten, wobei die Anfrage die Identifizierung einer kryptographischen Implementierung und Sicherheitsanforderungen für die kryptographische Implementierung für den Export durch den zweiten Korrespondenten umfasst, die zweite kryptographische Suite-Management-Einheit konfiguriert ist, um die kryptographische Implementierung bereitzustellen, die unter Verwendung der Sicherheitsanforderungen konfiguriert wurde und die konfigurierte kryptographische Implementierung zu dem ersten Korrespondenten zu exportieren, um es der ersten kryptographischen Suite-Management-Einheit zu ermöglichen, die konfigurierte kryptographische Implementierung für die Verwendung durch den ersten Korrespondenten sicher zu importieren.
21. System nach Anspruch 20, wobei der zweite Korrespondent ferner auf identische Weise wie bei der Interaktion zwischen dem ersten Korrespondenten und dem zweiten Korrespondenten mit einem dritten Korrespondenten kommuniziert, wobei der zweite Korrespondent ein vertrauenswürdiger Drittmittler ist, der die sichere Kommunikation zwischen dem ersten Korrespondenten und dem dritten Korrespondenten erleichtert.
22. System nach Anspruch 20, wobei jede kryptographische Suite-Management-Einheit konfiguriert ist, um eine Vielzahl kryptographischer Implementierungen für die Verwendung in einem gesicherten Suite-Tresor zu speichern und sie zu anderen Korrespondenten zu exportieren.
23. System nach Anspruch 22, wobei jede kryptographische Suite-Management-Einheit konfiguriert ist, um jede der Vielzahl von kryptographischen Implementierungen in ihrem Suite-Tresor zur Verwendung in einer sicheren Kommunikation dynamisch zu laden.
24. System nach Anspruch 22, wobei der Suite-Tresor jede kryptographische Implementierung während der Speicherung verschlüsselt und eine Kopie der für die Verschlüsselung verwendeten Schlüssel speichert.
25. System nach Anspruch 24, wobei der Suite-Tresor nach einer Anfrage zum Erhalt der kryptographischen Implementierung die verschlüsselte kryptographische Implementierung und die Schlüssel erhält, die kryptographische Implementierung unter Verwendung der Schlüssel entschlüsselt, die Schlüssel sicher löscht, die kryptographische Implementierung in einem flüchtigen Speicher auf eine virtuelle Disk schreibt, die kryptographische Implementierung für eine anfragende Anwendung verfügbar macht und die kryptographische Implementierung von der virtuellen Disk entfernt.
26. System nach Anspruch 20, wobei die Anfrage und der Export als ein Protokoll strukturiert sind, das kryptographische und Sicherheitsanforderungen von Importern und Exportern sicher verhandelt.
27. System nach Anspruch 26, wobei das Protokoll ein Public-Key-Verschlüsselungsverfahren verwendet und Folgendes umfasst:

a. der erste Korrespondent sendet eine Importanfrage, umfassend seinen Public Key, das Sicherheitsniveau seiner Anwendung und das für den kryptographischen Provider zu erwartende Sicherheitsniveau sowie die Plattform, an den zweiten Korrespondenten;

b. der zweite Korrespondent analysiert die Anfrage unter Berücksichtigung des Sicherheitsniveaus seiner Anwendung und seiner Richtlinie für das kryptographische Suite-Management, sucht durch seine kryptographischen Provider nach einer Übereinstimmung und entscheidet, ob der Export durchgeführt werden soll oder nicht;

c. nachdem sich der zweite Korrespondent für den Export entschieden hat, erzeugt der zweite Korrespondent ein Exportpaket, umfassend:

   i. seinen Public Key;

   ii. das Sicherheitsniveau seiner Anwendung;

   iii. Informationen über die kryptographische Implementierung und die Implementierung;

   iv. die kryptographische Implementierung, verschlüsselt mit dem Public Key des ersten Korrespondenten und, falls nötig, dem Private Key des zweiten Korrespondenten;

d. das Paket wird zu dem ersten Korrespondenten exportiert;

e. der erste Korrespondent empfängt das Paket, extrahiert die Informationen und entscheidet - auf Grundlage der Informationen und seiner Managementrichtlinie -, ob er annehmen soll oder nicht;

f. der erste Korrespondent entschlüsselt die kryptographische Implementierung mit dem Private Key des zweien Korrespondenten und, falls nötig, dem Public Key des zweiten Korrespondenten.

28. System nach Anspruch 27, wobei das Public-Key-Verschlüsselungsverfahren ECIES (Elliptic Curve Integrated Encryption Scheme) ist.

29. Verfahren nach Anspruch 28, umfassend eine Registrierungsphase, wenn die ersten und zweiten Komponenten Endpunkte sind, wobei jeder Endpunkt seine kryptographische Implementierung zu der kryptographischen Suite-Management-Einheit exportiert, welche ein Vermittler in dem Kommunikationskanal zwischen den beiden Endpunkten ist, gefolgt von der Ausführung eines Schlüsselzustimmungsprotokolls zur Generierung symmetrischer Schlüssel für jedes der zwei Paare, umfassend die kryptographische Suite-Management-Einheit und jeden der Endpunkte.

30. Verfahren nach Anspruch 29, umfassend den Dienst der Übersetzung von Chiffretexten, die von einem ersten Endpunkt erzeugt wurden, in Chiffretexte des anderen zweiten Endpunkts.

31. Verfahren nach Anspruch 30, wobei der Übersetzungsdienst Folgendes umfasst:

a. den ersten Endpunkt, der einen Klartext mit seinem symmetrischen Verschlüsselungsverfahren und dem Schlüssel, der zwischen dem ersten Endpunkt und der kryptographischen Suite-Management-Einheit während der Registrierung eingeführt wurde, verschlüsselt;

b. Übertragen des resultierenden Chiffretexts an die kryptographische Suite-Management-Einheit;

c. die kryptographische Suite-Management-Einheit, die den resultierenden Chiffretext mit dem Verschlüsselungs-/Entschlüsselungsverfahren des ersten Endpunkts und dem während der Registrierung eingeführten Schlüssel entschlüsselt, den resultierenden Klartext mit dem Verschlüsselungssystem des zweiten Endpunkts und dem zwischen dem zweiten Endpunkt und der kryptographischen Suite-Management-Einheit während der Registrierung eingeführten Schlüssel verschlüsselt und den resultierenden Chiffretext an den zweiten Endpunkt sendet;

d. den zweiten Endpunkt, der den empfangenen Chiffretext mit seinem Entschlüsselungsverfahren und dem Schlüssel, der zwischen dem zweiten Endpunkt und der kryptographischen Suite-Management-Einheit während der Registrierung eingeführt wurde, entschlüsselt.

32. System nach Anspruch 20, wobei die kryptographische Suite-Management-Einheit ein dynamisches Linken kryptographischer Implementierungen für Anwendungen, die an den Korrespondenten ausgeführt werden, bereitstellt.

33. System nach Anspruch 20, wobei die kryptographische Suite-Management-Einheit die Integrität der kryptographischen Implementierungen sicherstellt, die für anfragende Anwendungen verfügbar gemacht werden.

34. System nach Anspruch 20, wobei die zweite kryptographische Suite-Management-Einheit konfiguriert ist, um Richtlinien festzulegen, die Nutzungsbedingungen der kryptographischen Implementierung bestimmen.

35. System nach Anspruch 34, wobei die Richtlinien Lizenzbedingungen umfassen, die Anwendungen und Geräte festlegen, denen eine Verwendung der kryptographischen Implementierung erlaubt ist.

36. System nach Anspruch 34, wobei die Richtlinien Lizenzbedingungen umfassen, die den Zeitrahmen festlegen, in dem die kryptographische Implementierung genutzt werden darf.

37. System nach Anspruch 34, wobei nach dem Versuch einer Anwendung oder eines Geräts, eine kryptographische Implementierung auf unerlaubte Weise zu verwenden, die kryptographische Suite-Management-Einheit die kryptographische Implementierung aus dem Suite-Tresor löscht.

38. System nach Anspruch 20, wobei der erste Korrespondent seinen Public Key in der Anfrage bereitstellt.

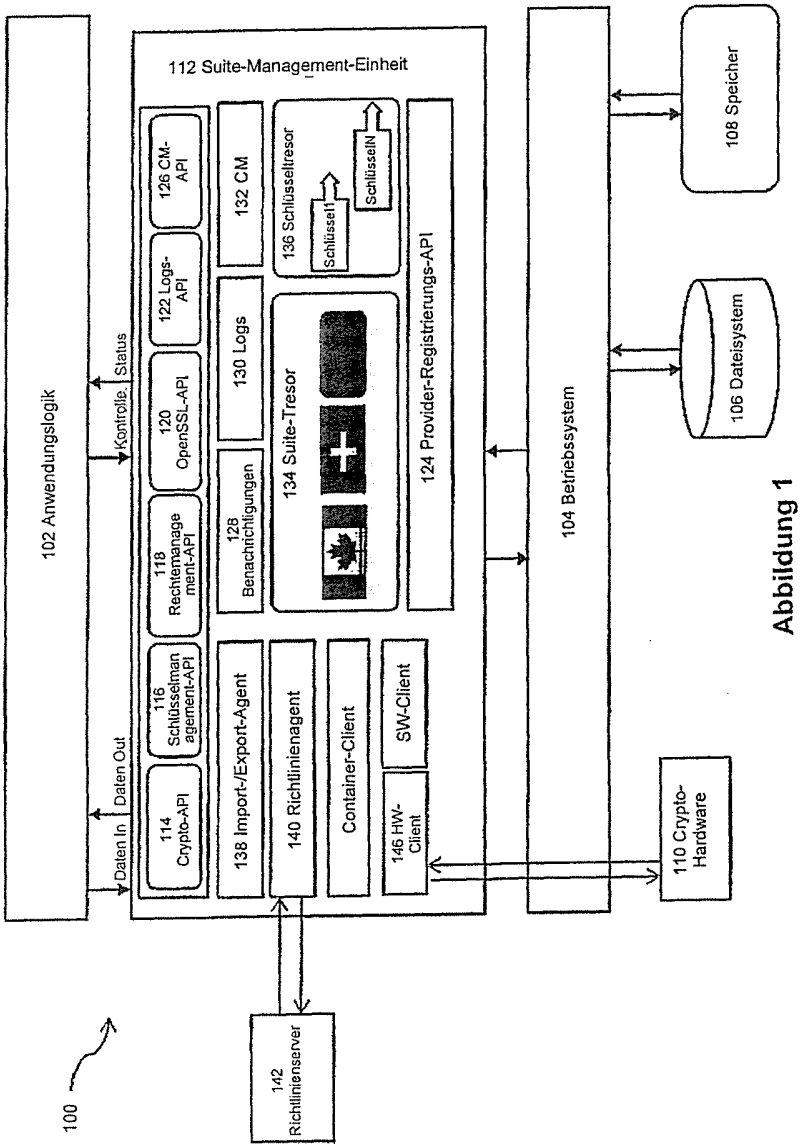

100
102 Anwendungslogik
112 Suite-Management-Einheit
Daten In
Daten Out
Kontrolle
Status
114 Crypto-API
116 Schlüsselmanagement-API
118 Rechtemanagement-API
120 OpenSSL-API
122 Logs-API
126 CM-API
138 Import-/Export-Agent
140 Richtlinienagent
Container-Client
146 HW-Client
SW-Client
128 Benachrichtigungen
130 Logs
132 CM
134 Suite-Tresor
136 Schlüsseltresor
Schlüssel1
SchlüsselN
124 Provider-Registrierungs-API
104 Betriebssystem
108 Speicher
106 Dateisystem
110 Crypto-Hardware
142 Richtlinienserver

Abbildung 1

148 CipherMgtApi
154 Import Request
156 GetImportRequest
160 ImportBundle
158 ExportBundle
126 ConfigMgrApi
162 RegisterBundle
164 RemoveBundle
166 ListBundles
150 KeyVaultApi
168 GenerateKeyPair
170 GetPrivateKey
152 SuiteVaultApi
172 StoreBundle
174 RemoveBundle
176 LoadBundle
178 UnLoadBundle
180 ValidateBundles

Abbildung 2

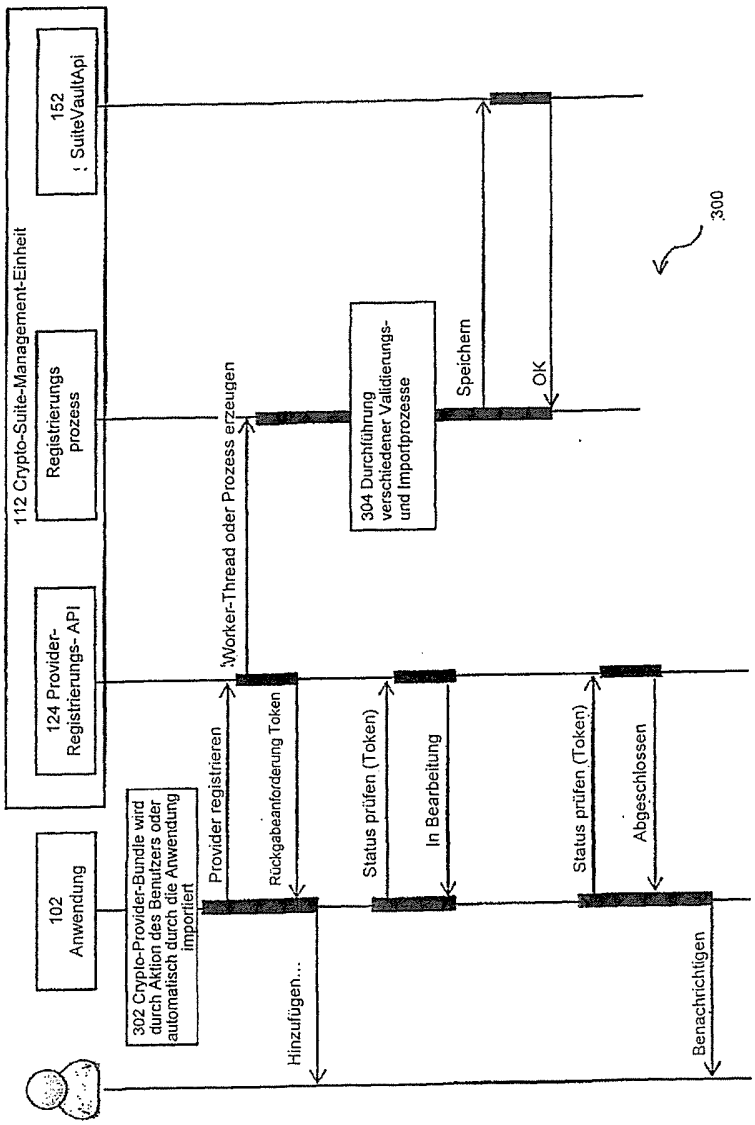

300
112 Crypto-Suite-Management-Einheit
152 : SuiteVaultApi
Registrierungs prozess
124 Provider-Registrierungs- API
102 Anwendung
302 Crypto-Provider-Bundle wird durch Aktion des Benutzers oder automatisch durch die Anwendung importiert
Provider registrieren
Worker-Thread oder Prozess erzeugen
Rückgabeanforderung Token
304 Durchführung verschiedener Validierungs- und Importprozesse
Speichern
OK
Status prüfen (Token)
In Bearbeitung
Status prüfen (Token)
Abgeschlossen
Hinzufügen...
Benachrichtigen

Abbildung 3

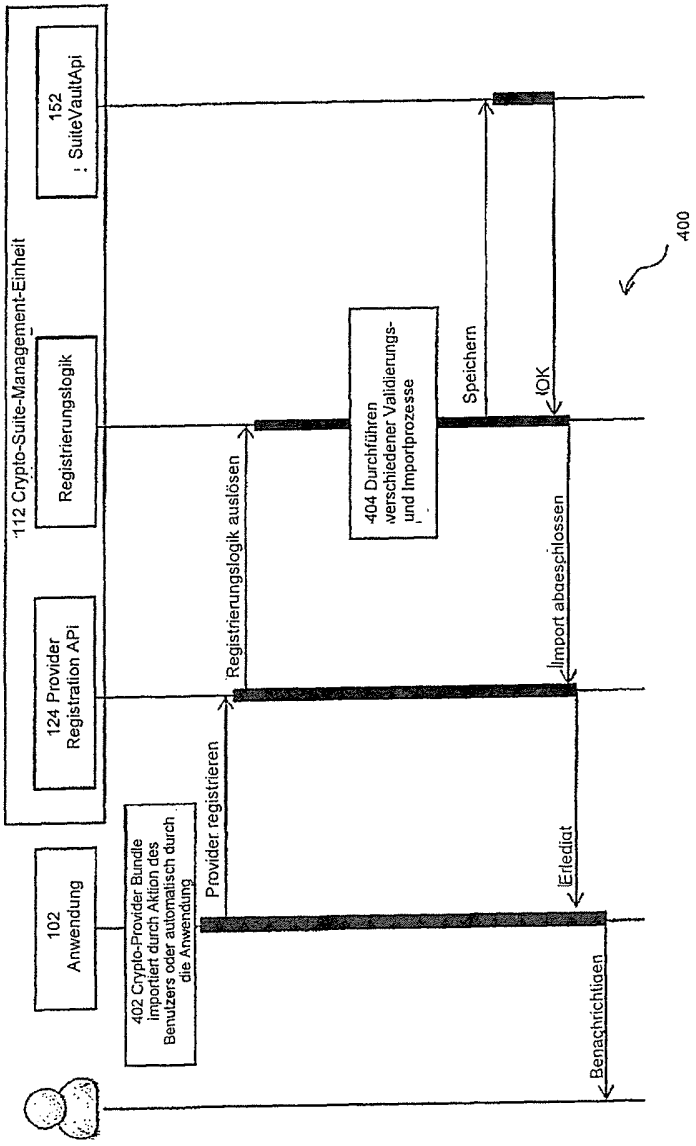

112 Crypto-Suite-Management-Einheit
152
: SuiteVaultApi
Registrierungslogik
124 Provider
Registration APi
102
Anwendung
402 Crypto-Provider Bundle
importiert durch Aktion des
Benutzers oder automatisch durch
die Anwendung
Provider registrieren
Registrierungslogik auslösen
404 Durchführen
verschiedener Validierungs-
und Importprozesse
Speichern
OK
Import abgeschlossen
Erledigt
Benachrichtigen
400

Abbildung 4

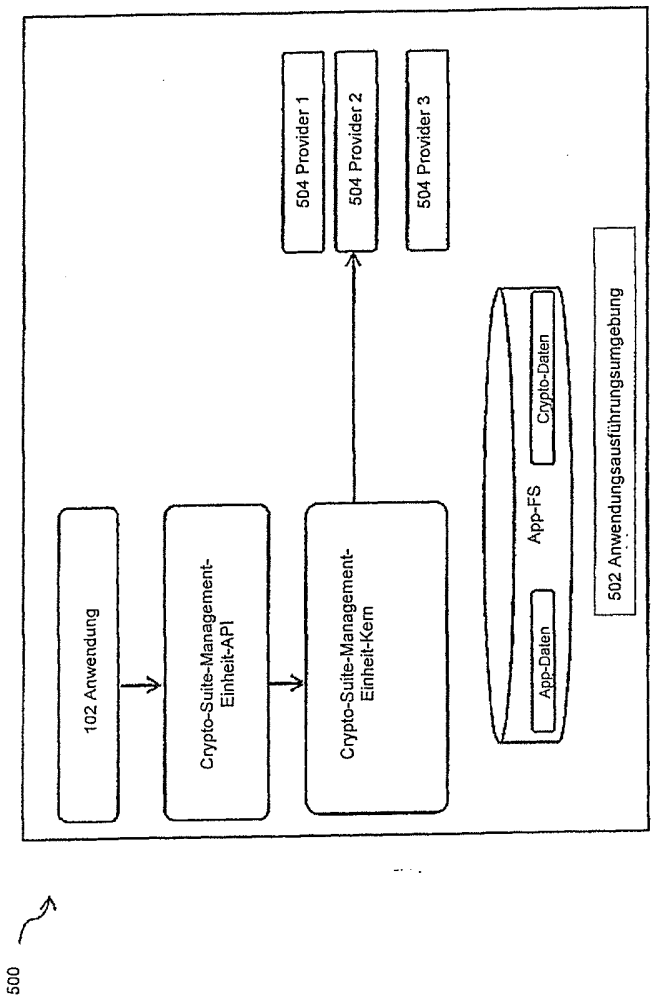

500
102 Anwendung
Crypto-Suite-Management-Einheit-API
Crypto-Suite-Management-Einheit-Kern
504 Provider 1
504 Provider 2
504 Provider 3
App-FS
App-Daten
Crypto-Daten
502 Anwendungsausführungsumgebung

Abbildung 5

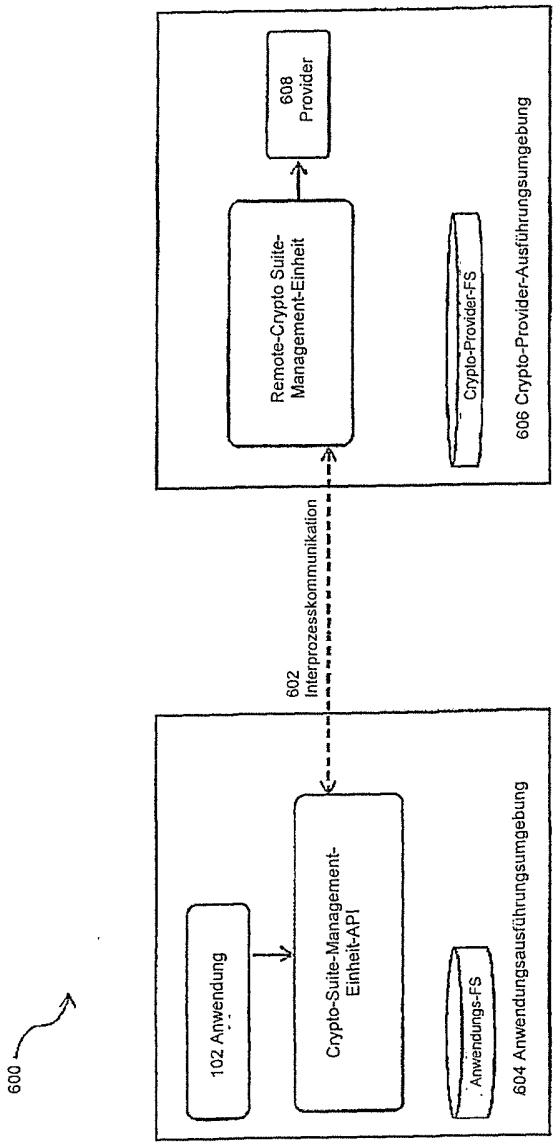

600
102 Anwendung
Crypto-Suite-Management-Einheit-API
Anwendungs-FS
604 Anwendungsausführungsumgebung
602
Interprozesskommunikation
Remote-Crypto Suite-Management-Einheit
608 Provider
Crypto-Provider-FS
606 Crypto-Provider-Ausführungsumgebung

Abbildung 6

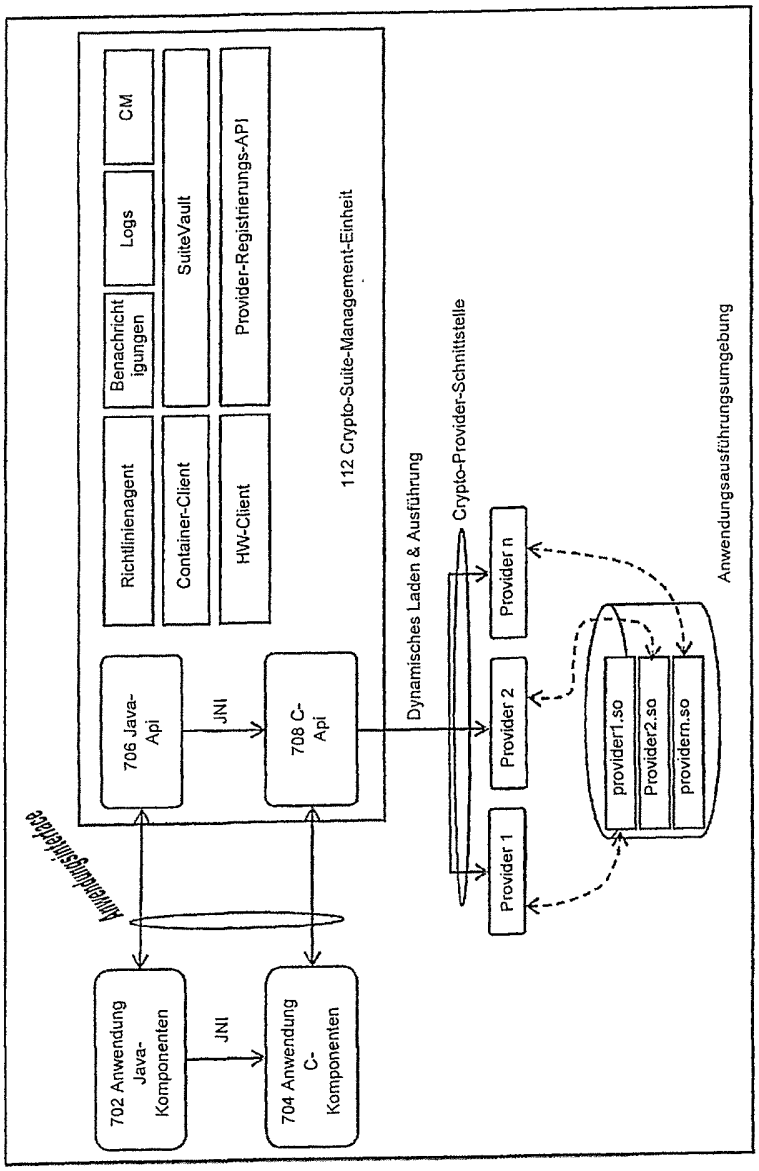

Anwendungsschnittstelle
702 Anwendung Java-Komponenten
JNI
704 Anwendung C-Komponenten
706 Java-Api
JNI
708 C-Api
112 Crypto-Suite-Management-Einheit
Richtlinienagent
Container-Client
HW-Client
Benachrichtigungen
Logs
CM
SuiteVault
Provider-Registrierungs-API
Dynamisches Laden & Ausführung
Crypto-Provider-Schnittstelle
Provider 1
Provider 2
Provider n
provider1.so
Provider2.so
providern.so
Anwendungsausführungsumgebung

Abbildung 7

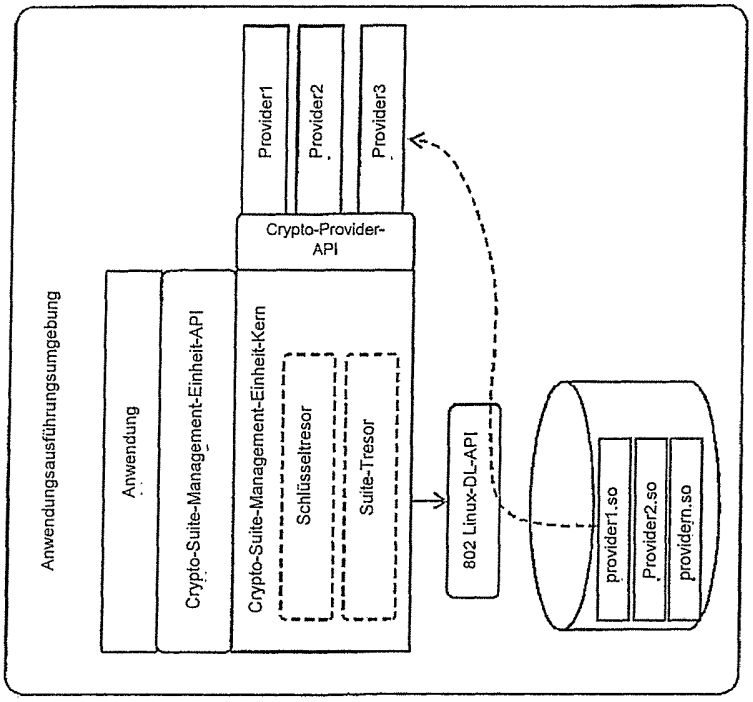

Anwendungsausführungsumgebung
Anwendung
Crypto-Suite-Management-Einheit-API
Crypto-Suite-Management-Einheit-Kern
Schlüsseltresor
Suite-Tresor
Crypto-Provider-API
Provider1
Provider2
Provider3
802 Linux-DL-API
provider1.so
Provider2.so
providern.so

Abbildung 8

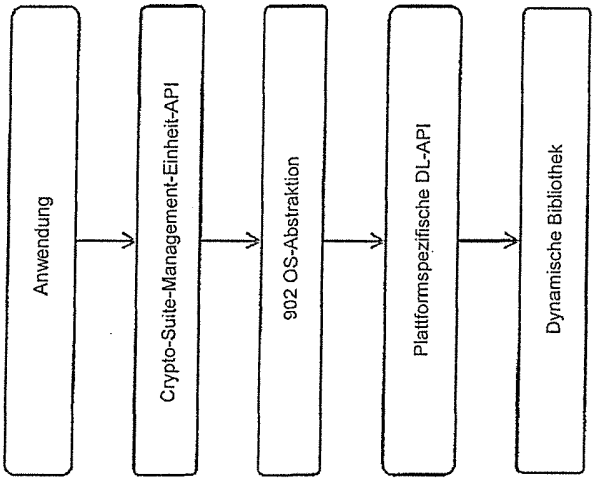

Anwendung
Crypto-Suite-Management-Einheit-API
902 OS-Abstraktion
Plattformspezifische DL-API
Dynamische Bibliothek

Abbildung 9

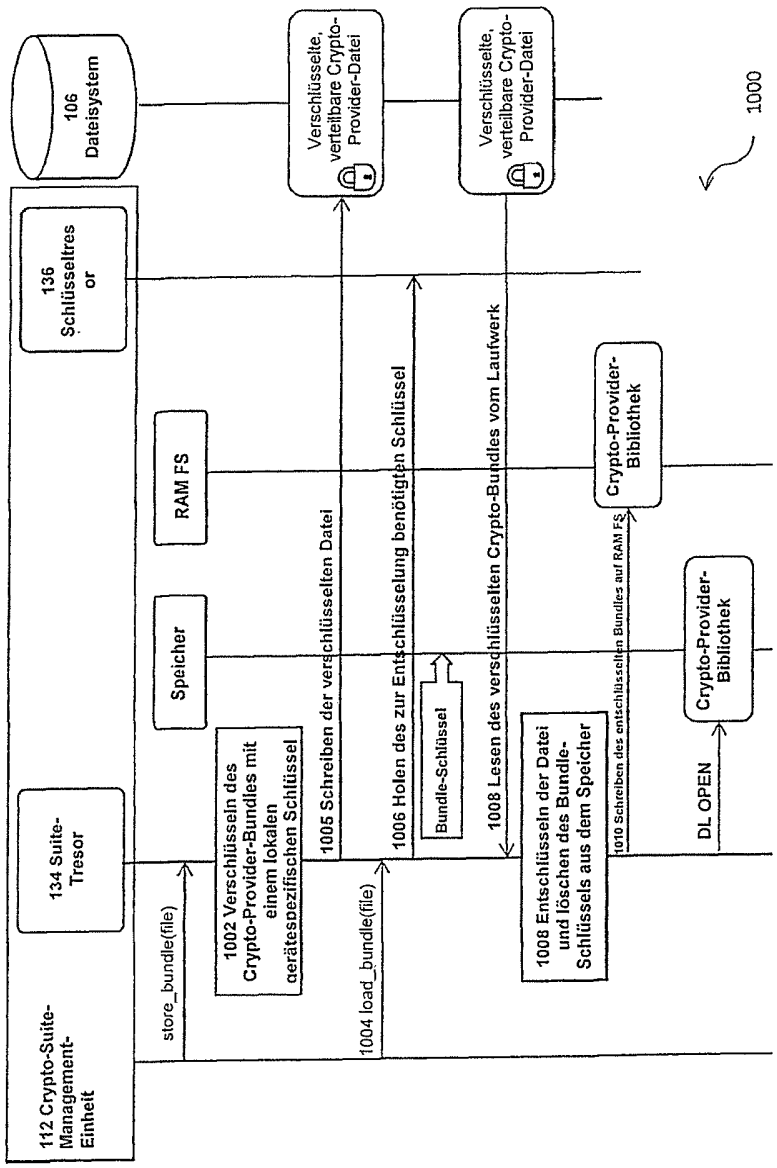


Abbildung 10

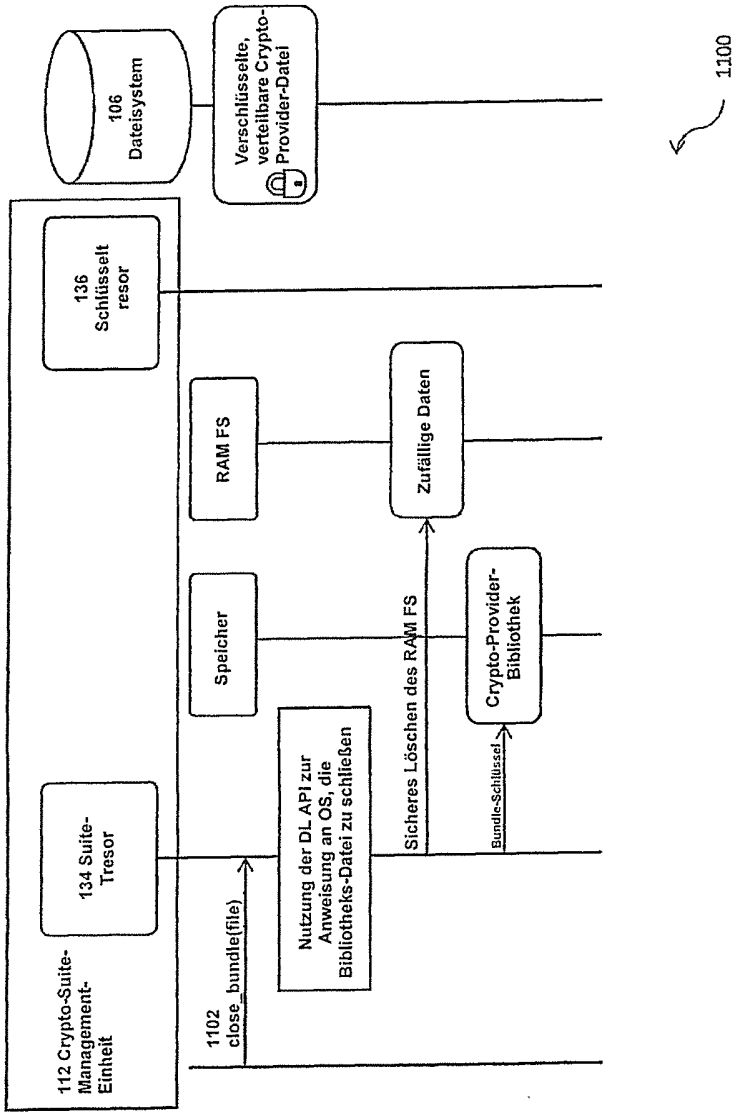


Abbildung 11

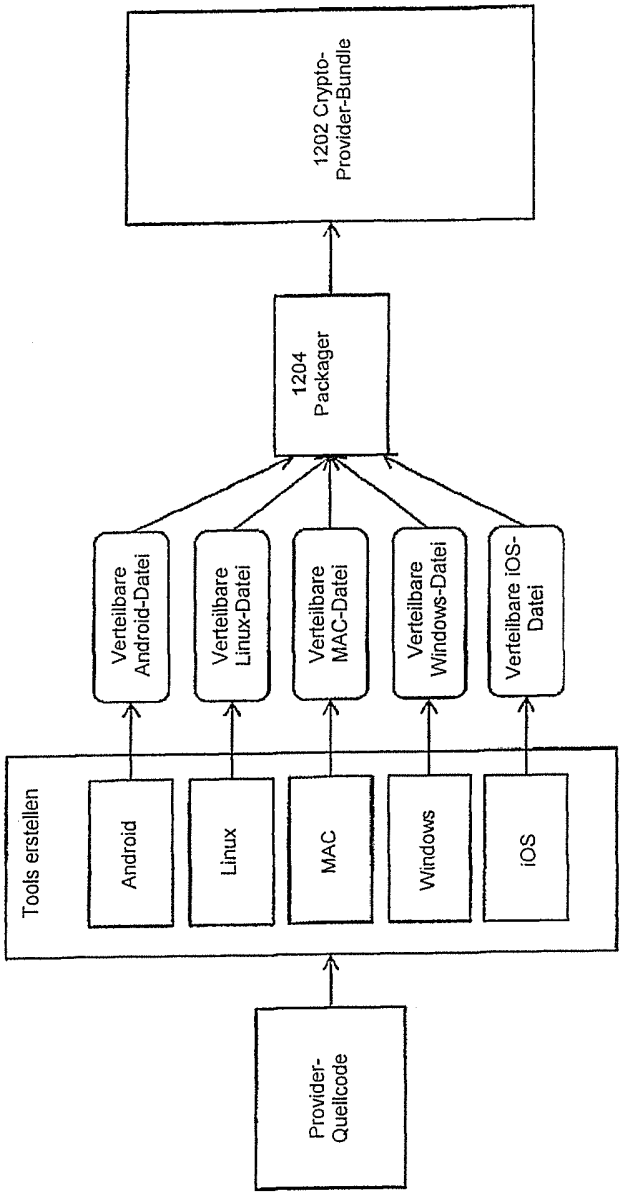


Abbildung 12

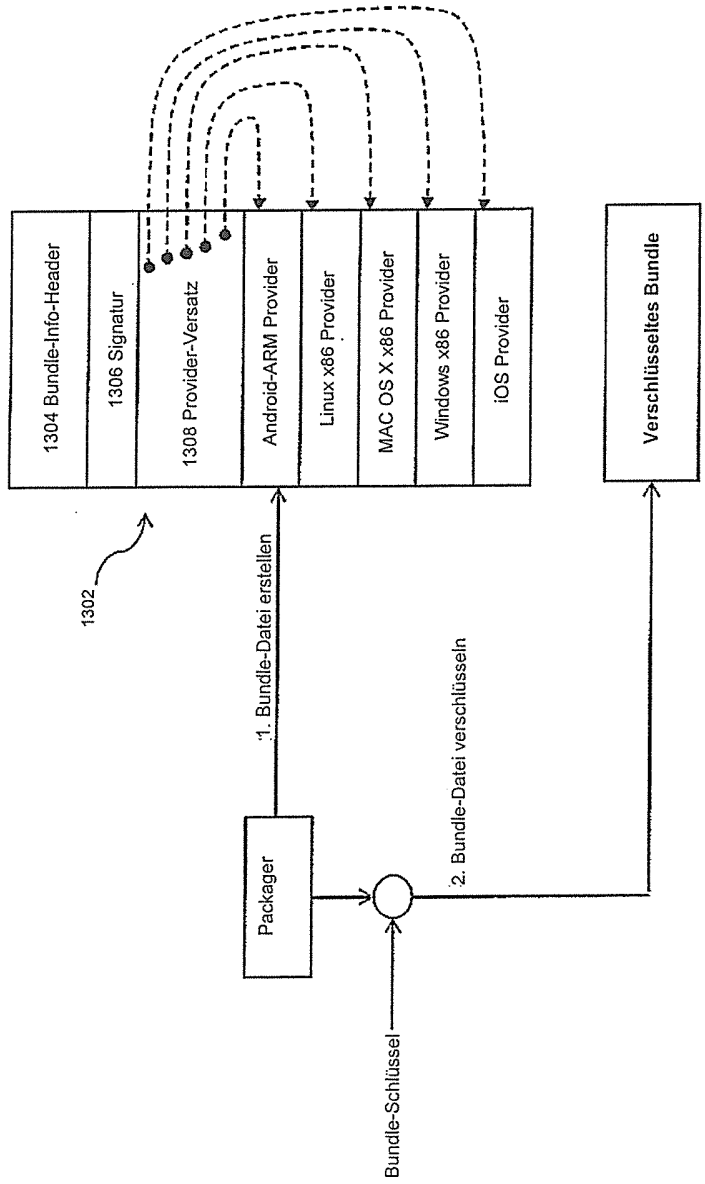


Abbildung 13

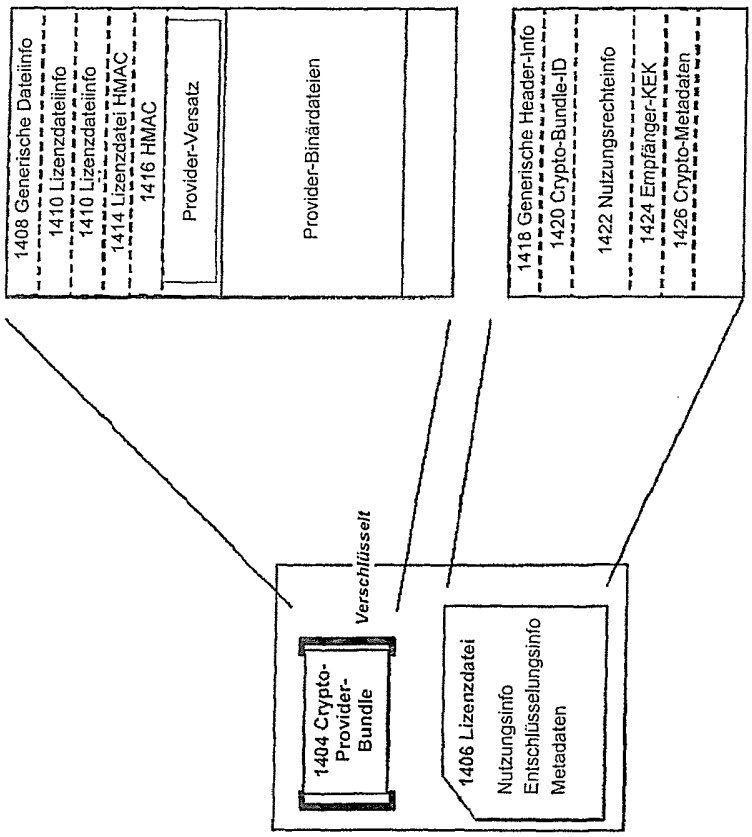


Abbildung 14

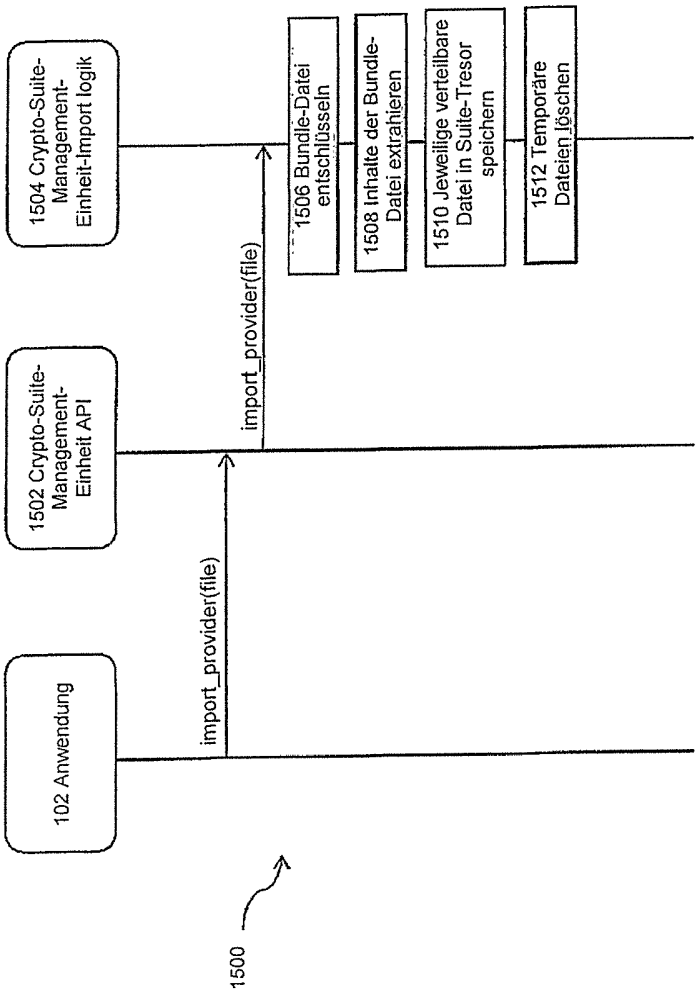


Abbildung 15

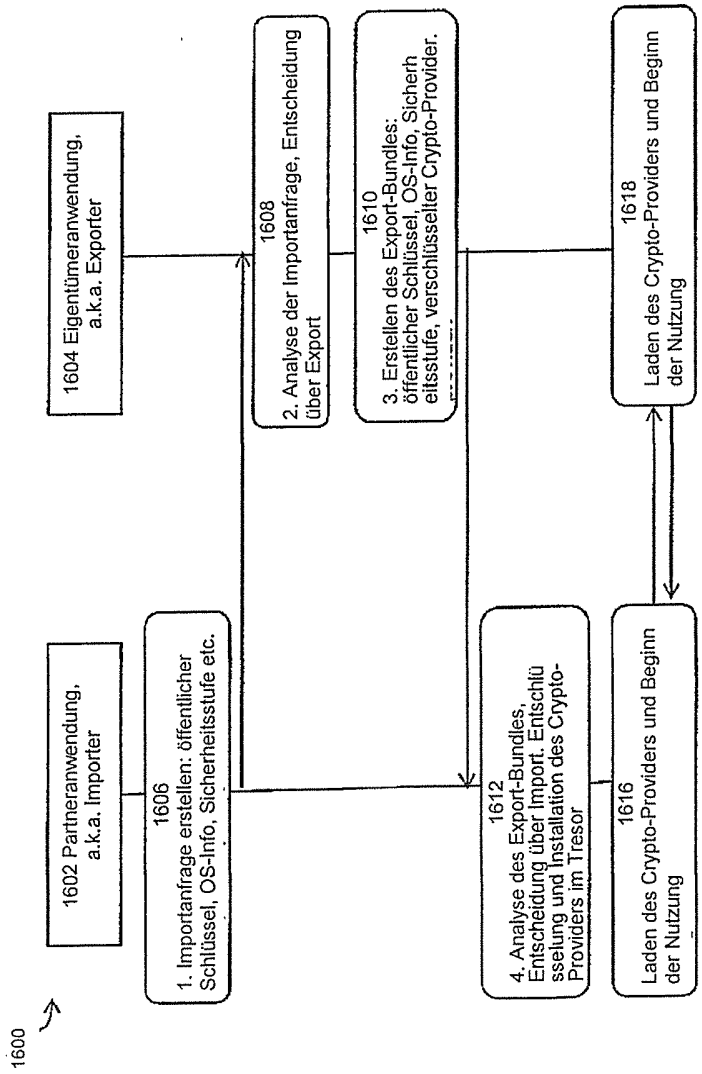


Abbildung 16

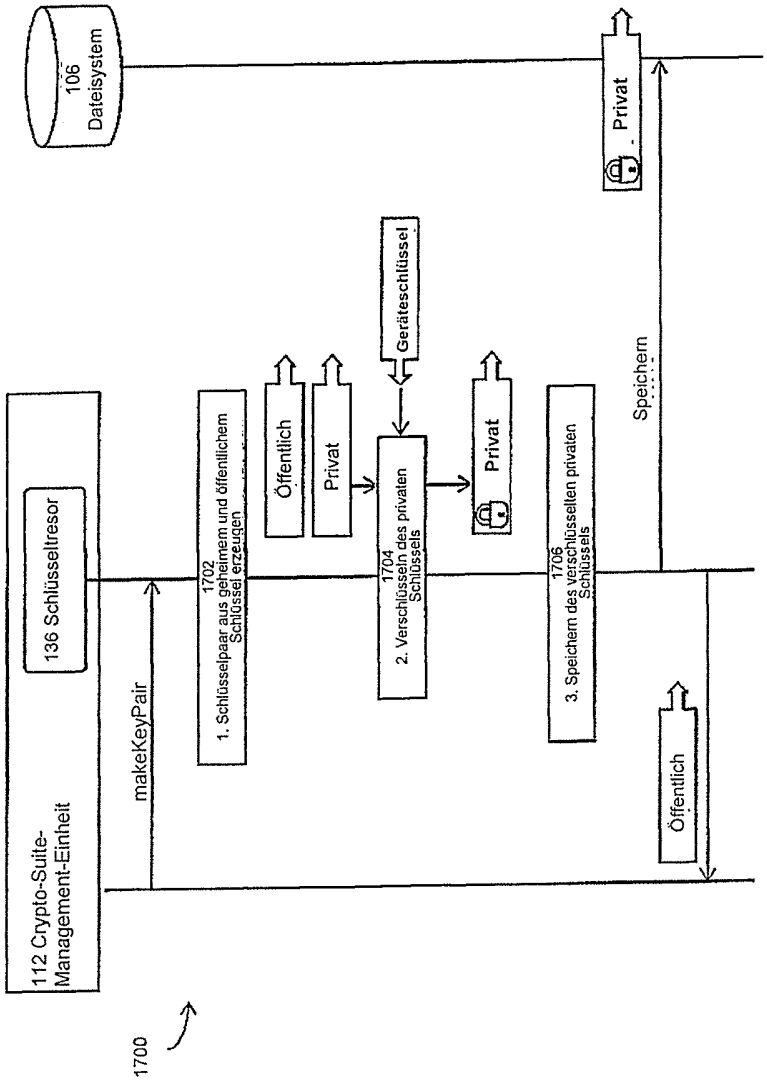


Abbildung 17

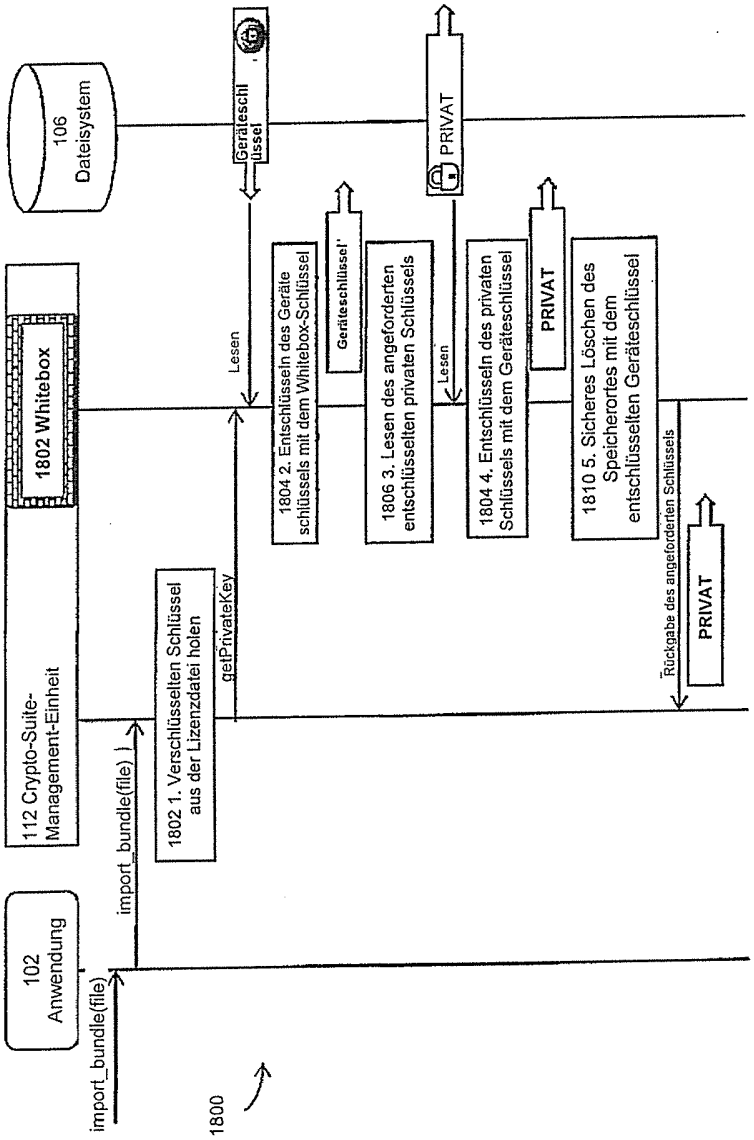


Abbildung 18

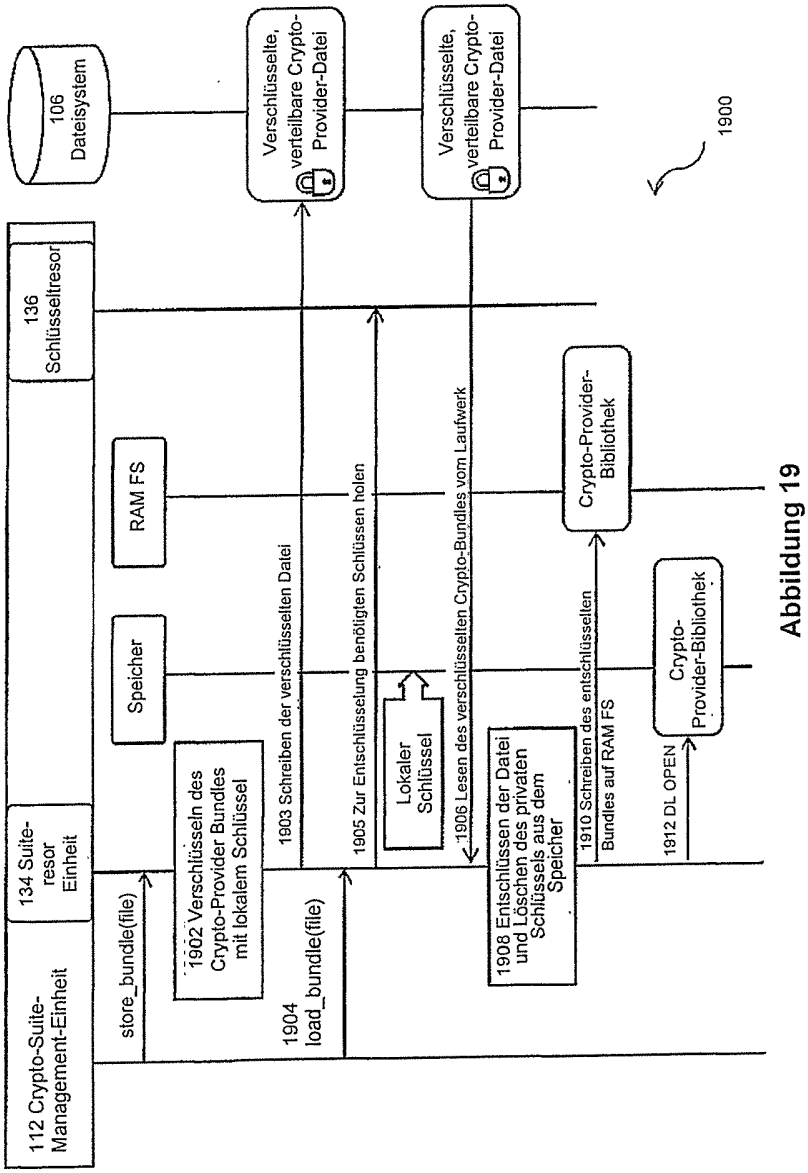


Abbildung 19

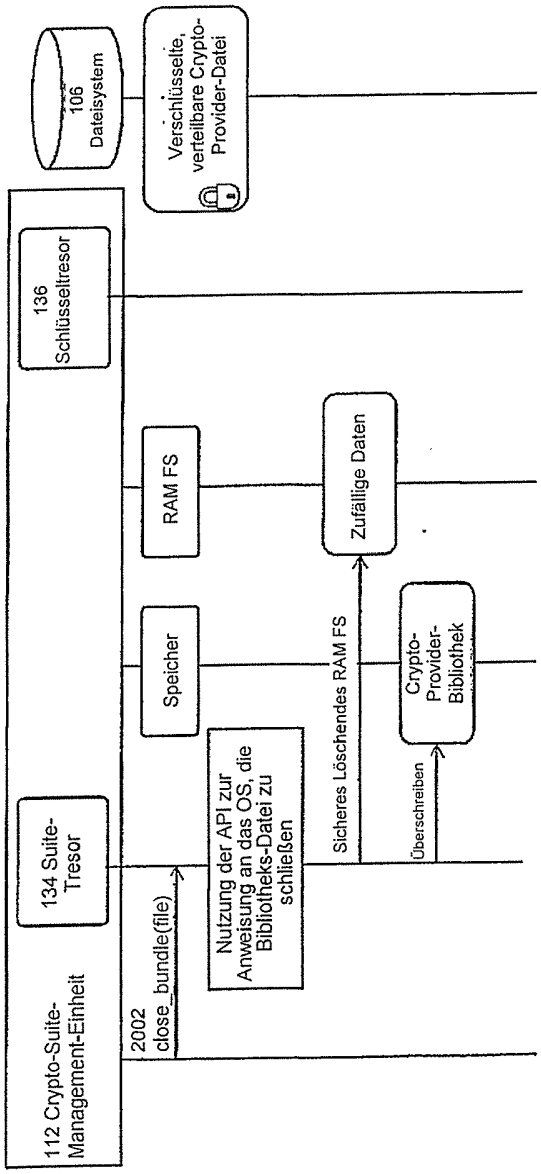


Abbildung 20

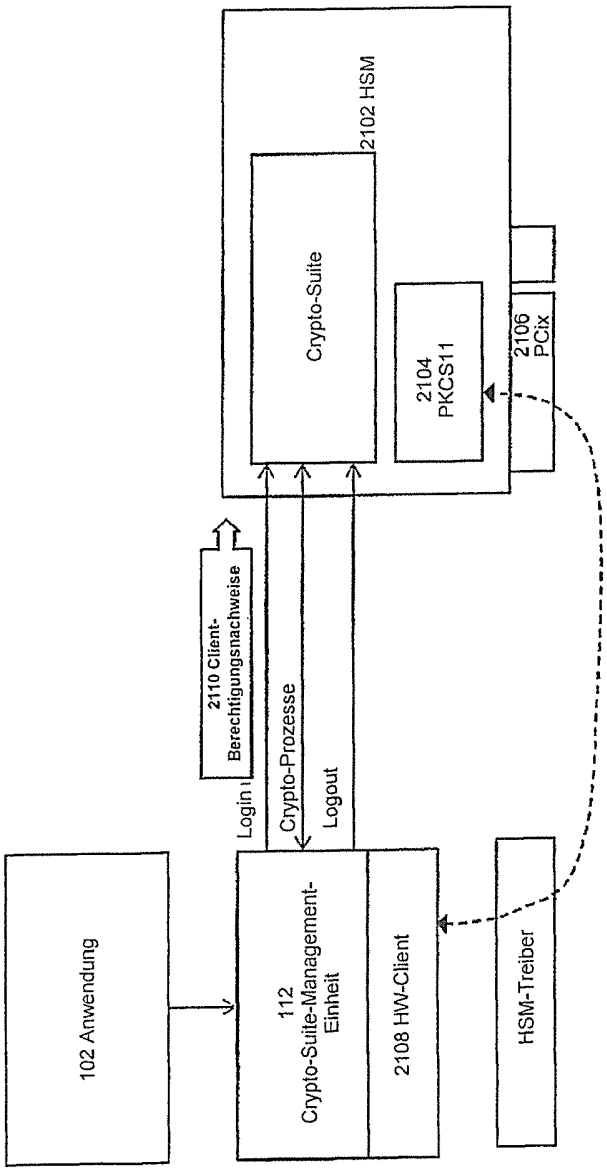


Abbildung 21

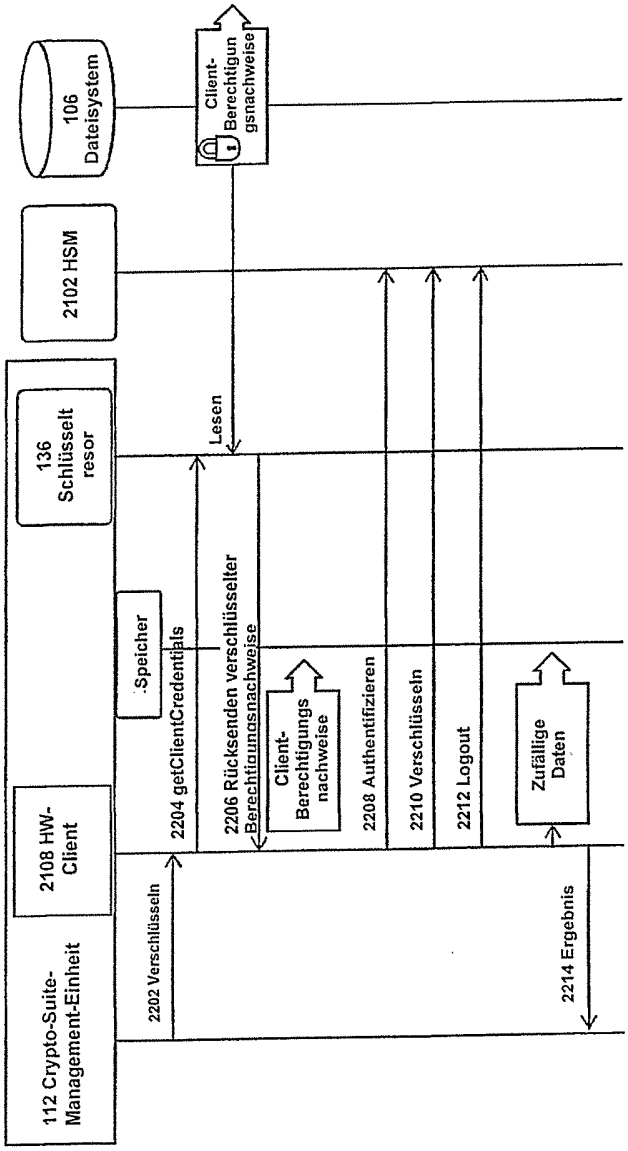


Abbildung 22

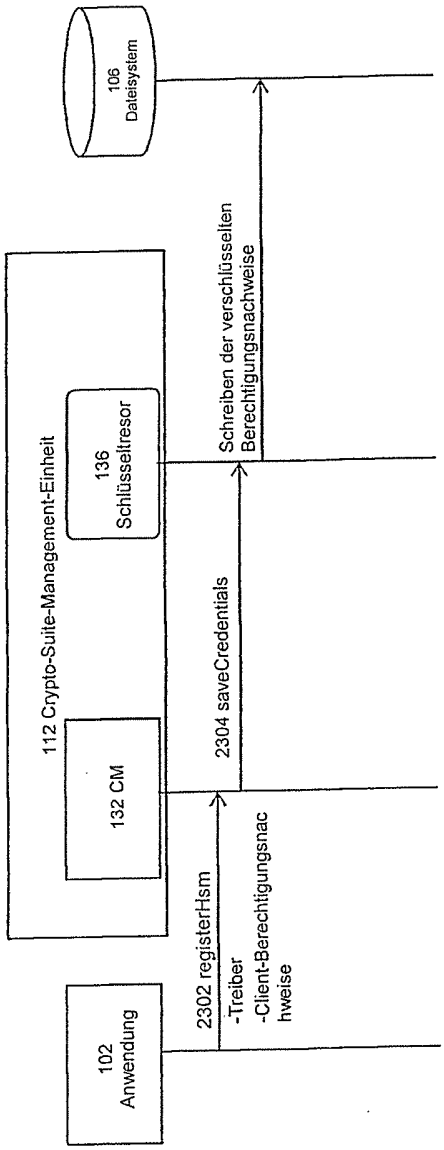


Abbildung 23

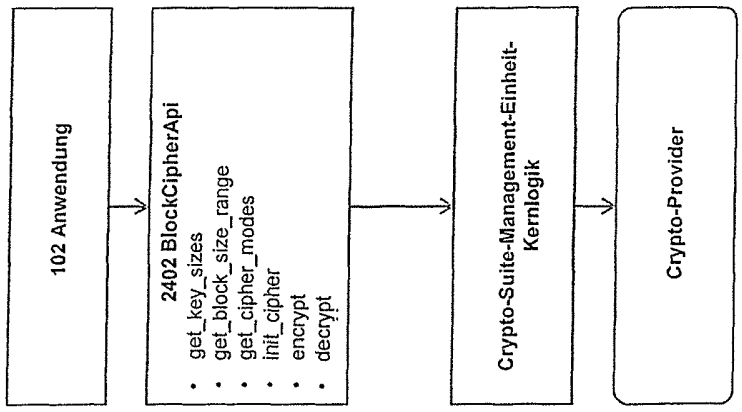


Abbildung 24

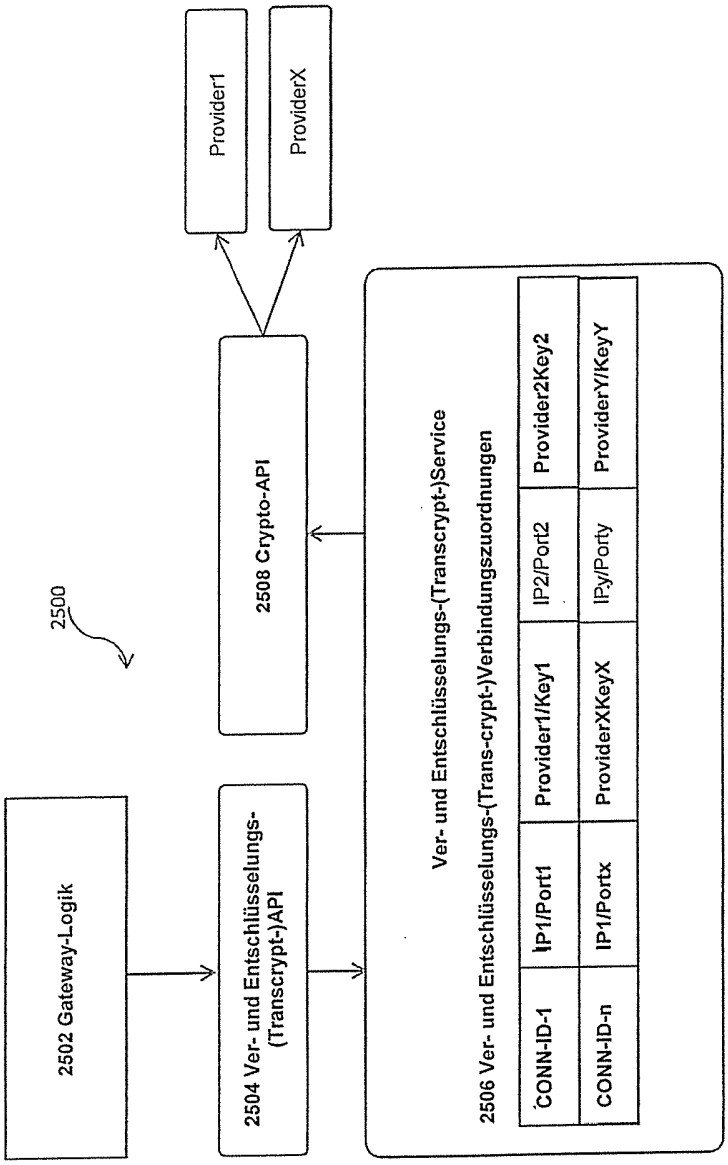


Abbildung 25

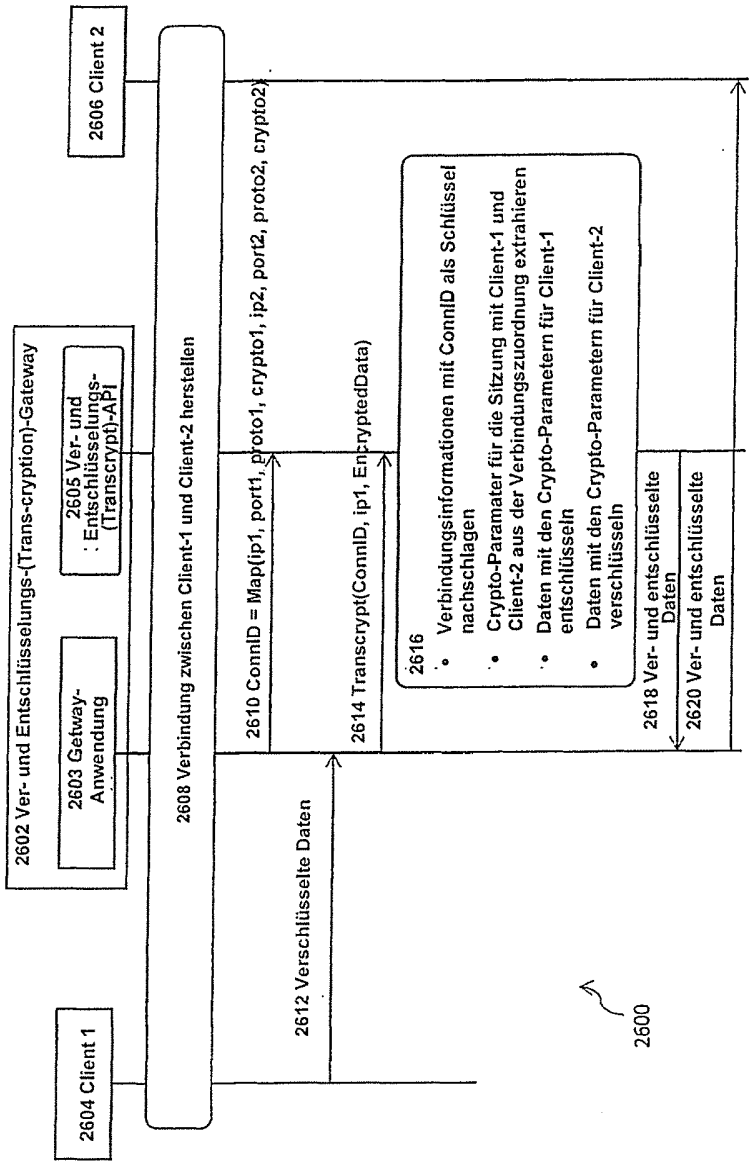


Abbildung 26

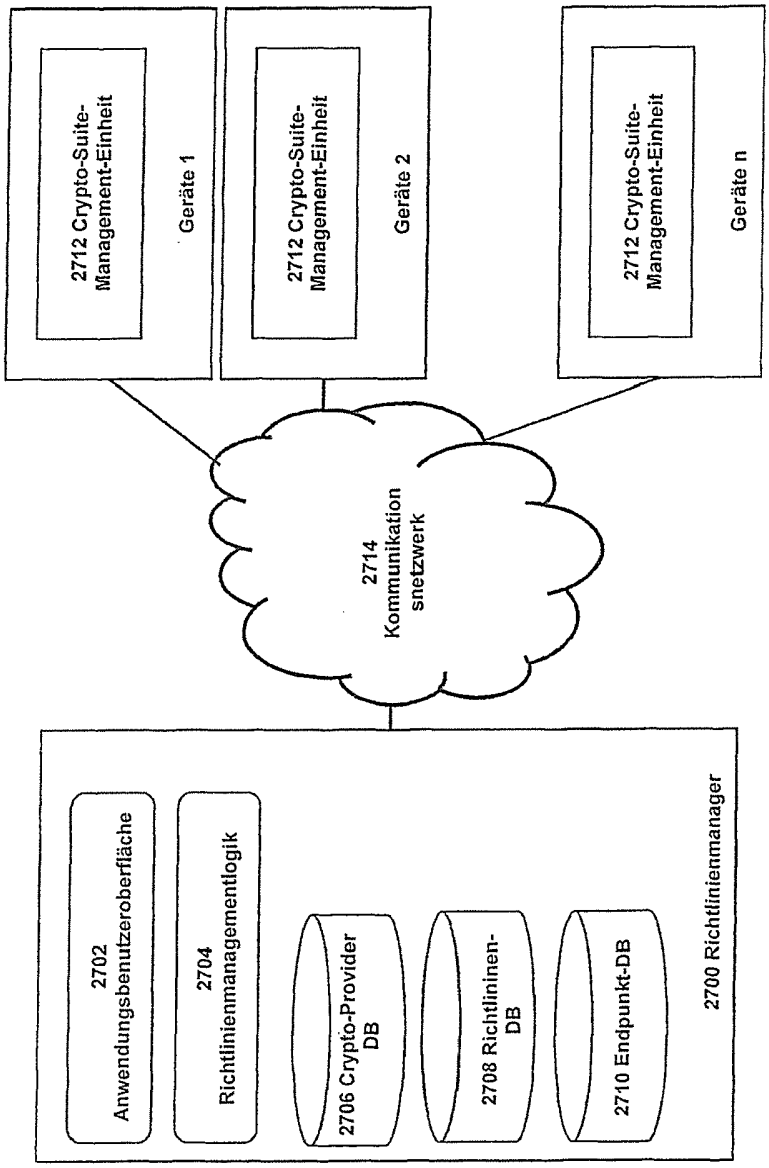


Abbildung 27