(19) österreichisches patentamt

(10) **AT 522816 A1 2021-02-15**

(12) **Österreichische Patentanmeldung**

(21) Anmeldenummer: A 267/2019
(22) Anmeldetag: 02.08.2019
(43) Veröffentlicht am: 15.02.2021

(51) Int. Cl.: ***G06F 21/12*** (2013.01)
G06F 21/44 (2013.01)
G06F 21/45 (2013.01)
H04L 9/00 (2006.01)
H04L 9/08 (2006.01)

(56) Entgegenhaltungen:
US 2019080091 A1
EP 3337119 A1
WO 2018183926 A1
US 2018129801 A1
VIANAYAKRAY-JANI et al. “Security Architecture for Cluster based Ad Hoc Networks” 06.07.2012; abgerufen im Internet am 10.06.2020 unter dem Link:<http://www.tifr.res.in/~sanyal/papers/Security_Architecture_for_Cluster_based_Ad_Hoc_Networks.pdf>

(71) Patentanmelder:
CRYPTAS it-Security GmbH
1030 Wien (AT)

(72) Erfinder:
Bumerl Stefan Dipl.Ing. (FH)
1030 Wien (AT)
Tillich Stefan Dr.
3500 Krems an der Donau (AT)
Rössler Thomas Dr.
8047 Hart bei Graz (AT)

(74) Vertreter:
Patentanwälte Puchberger & Partner
1010 Wien (AT)

AT 522816 A1 2021-02-15

(54) **Verfahren zur performanten Durchführung von kryptographischen Einzeloperationen**

(57) Die Erfindung betrifft ein Verfahren zur Nutzung eines Verbunds (Cluster) von kryptographischen Sicherheitselementen, wobei für die performante Durchführung von kryptographischen Operationen ein Verbund (Cluster) aus kryptographischen Sicherheitselementen elastisch genutzt werden, indem auf deren Einzelelemente die erforderlichen kryptographischen Einzeloperationen agil verteilt werden.

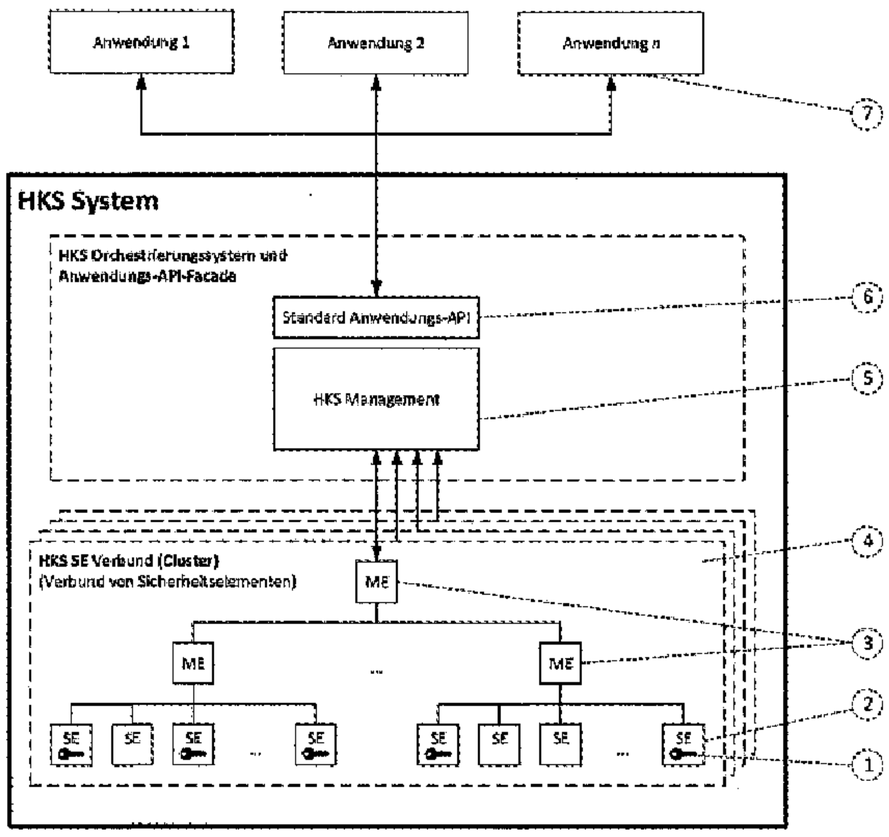

Fig. 1

Die Erfindung betrifft ein Verfahren zur Nutzung eines Verbunds (Cluster) von kryptographischen Sicherheitselementen, wobei für die performante Durchführung von kryptographischen Operationen ein Verbund (Cluster) aus kryptographischen Sicherheitselementen elastisch genutzt werden, indem auf deren Einzelelemente die erforderlichen kryptographischen Einzeloperationen agil verteilt werden.

Einleitung und Stand der Technik

Die Erfindung betrifft eine innovative Alternative zu traditionellen Hardware Security Modulen (HSM) auf Basis eines Verbunds von Hardware-Sicherheitselementen gemäß dem Oberbegriff des Anspruches 1.

Betrachtet man übliche Mehrzweck Hardware Security Module (HSM), die als kryptographisches Sicherheitselement etwa im Rahmen einer Public Key Infrastructure (PKI) oder in anderen Anwendungen (Payment, Signaturen, Ver-/Entschlüsselungssysteme etc.) zum Einsatz gebracht werden, so sind diese aufgrund deren Bauform, Kosten und meist eingeschränkten Funktionen nur in Großsystemen nutzbar und leistbar. Darüber hinaus lassen etablierte HSMs vor allem kaum elastische Betriebsformen zu, bei der etwa die Performanz von Krypto-Operationen je nach Bedarf in einen gewissen Rahmen dynamisch angepasst werden kann, etwa durch die automatische, sichere Verteilung des kryptographischen Schlüsselmaterials auf eine größerer Anzahl solcher Module. Dieser Art der Skalierung stehen auch wiederum die relativ hohen Kosten etablierter HSMs entgegen. Andererseits erheben aber gerade SaaS- und Cloud-Anwendungen vermehrt einen Bedarf für derart skalierbare kryptographische Sicherheitsmodule.

Es ist daher ein neuer und vor allem elastischer Ansatz erforderlich, um hardwarebasierte kryptographische Sicherheitsmodule aufzubauen, ohne dabei auf die hohe Sicherheit, wie von etablierten HSMs bekannt und von Anwendungen gefordert, zu verzichten. Der neue Ansatz muss aber auch für Kleinst- und Kleinanwendungen durchführbar sein und dem zur Folge im Gegensatz zu etablierten HSMs nicht nur in der Betriebseinführung sondern vor allem auch in der Betriebsführung möglichst autonom, selbstverwaltet und kompakt, und letztendlich kosteneffizient sein.

Etablierte HSMs entsprechen im Kern konventionellen Rechnerarchitekturen, deren Hardware sehr stark in Bezug auf die komplexen Anforderungen kryptographischer Algorithmen optimiert ist. Zudem verfügen sie über eine Vielzahl von Sicherheitsmechanismen. Der Aufbau ist jedoch makroskopisch und eignet sich nur bedingt zur Skalierung durch das Clustern mehrerer solcher HSMs.

Demgegenüber stehen sogenannte kryptographische Sicherheitselemente (Secure Elements) in Form von integrierten Schaltkreisen, die hochintegriert in Bezug auf einzelne kryptographische Funktionen eine vergleichbare oder sogar die selbe Sicherheit bieten wie etablierte HSMs, aber im Gegensatz zu HSMs in Massen produziert werden und daher weit verbreitet und günstig sind. Derartige Elemente sind in Smartcards heute weit verbreitet. Unser Ansatz geht daher davon aus, eine Vielzahl derartiger, günstiger Secure Elements im Verbund (Cluster) zu betreiben, um Krypto-Operationen performant, redundant und effizient abwickeln zu können.

Kryptographische Sicherheitselemente (Secure Elements) werden in Smartcards seit Jahrzehnten eingesetzt, etwa in den Anwendungsbereichen Payment, eID (Mitarbeiter-Ausweise oder Reisepass) oder bei elektronischen Signaturen (Signaturkarten). Für diese Anwendungsgebiete finden massenhaft

Sicherheitschips im Kartenformat, in den letzten Jahren aber auch vermehrt gepaart mit NFC Funktionalitäten in Smartphones, etwa für kontaktloses Zahlen, Anwendung. Diese Secure Elements sind ihrerseits hochspezialisierte Mikrocontroller, deren Komponenten für sichere kryptographische Operationen die notwendigen Algorithmen und Protokolle, sowie zum sicheren Speichern von Schlüsselmaterial entsprechend sichere Speicherelemente, implementiert haben. Zusätzlich verfügen sie über eine Reihe von Sicherheitsmechanismen, die verschiedenen Arten von Angriffen (Side-Channel-Attacken, etc.) entgegenwirken. Durch entsprechende Zertifizierungen bestätigen die Hersteller den hohen Sicherheitsstandard ihrer Sicherheitsmodule. Vorteile dieser Technologie: diese Elemente sind kostengünstig, weil solche Module in hohen Stückzahlen verfügbar sind; sie implementieren einen hohen Sicherheitslevel; sie sind sehr gut standardisiert und weisen eine breite Kompatibilität auf und verfügen über eine geringe Leistungsaufnahme. Die Nachteile dieser Technologie, wie die vergleichsweisen langsamen I/O-Interfaces der Elemente, die geringere Rechenleistung infolge der gewünschten minimalen Leistungsaufnahme sowie eine geringere Lebensdauer einzelner Elemente durch eine beschränkte Anzahl von Lese-/Schreibzyklen, sind besonders durch die Verwendung einer großen Anzahl von Elementen und durch ein geeignetes Orchestrierungsverfahren zu kompensieren. Ein derartiges, elastisches Orchestrierungsverfahren ist neu und steht im Fokus dieses Patentes.

Figurenaufzählung

Fig. 1 zeigt die Gesamtarchitektur des HKS-Systems.

Beschreibung

Das Hardware-Key-Store-Modul (HKS) ist eine innovative Alternative zu traditionellen Hardware Security Modulen (HSM). Marktübliche HSMs bieten zwar eine hohe funktionelle Sicherheit, sind aber andererseits sehr komplex und bedingen letztlich hohe Kosten, sowohl bei deren Anschaffung und Einführung als auch im Betrieb. Das HKS-Modul zeichnet hingegen insbesondere die Merkmal Elastizität und geringere Herstellungskosten aus, ohne allerdings Sicherheitseinbußen in Kauf nehmen zu müssen. Das HKS-Modul wird im Gegensatz zu konventionellen HSMs auf Basis handelsüblicher kryptographischer Secure Elements aufgebaut, die in großen Mengen in verschiedensten Anwendungen (z.B. Smart-Cards) bereits Verwendung finden und daher als Massenprodukt entsprechend kostengünstig verfügbar sind. Beim HKS-Modul werden einzelnen diese Secure Elements über eine logische Struktur (Cluster) miteinander verbunden und entsprechend orchestriert, um so eine Alternative zu marktüblichen HSMs zu erhalten, die ausfallsicher, performant und hoch skalierbar ist.

Die Sicherheit des HKS-Moduls wird bereits durch die einzelnen Secure Elements des Clusters gewährleistetet, da diese schon höchste Sicherheitsstandards erfüllen. Die Skalierbarkeit und Ausfallssicherheit wird durch die von uns eingeführte logische Struktur und Orchestrierungsweise gewährleistet. Die schützenswerten, kryptographischen Schlüsselinformationen bleiben so entweder in den

Secure Elements oder werden innerhalb der logischen Struktur nur über Secure Messaging ausgetauscht. Ein unverschlüsselt exportiert von Schlüsselmaterial oder dessen unberechtigte Nutzung ist somit nicht möglich.

Die Struktur aus einer Vielzahl an Secure Elements wird durch das HKS-Management orchestriert. Der durch das HKS gebildete Cluster an Secure Elements bietet nach außen hin nur einen einzelnen Kontaktpunkt, um in bestehende Anwendungen an Stelle eines klassischen HSMs einfach integriert werden zu können. Das HKS-Management abstrahiert über dies hinaus die dahinterliegende Struktur derartig, sodass die technischen Parameter zur Generierung, Speicherung und Anwendung von kryptografischem Material sowie die Auswahl von zu verwendenden Secure Elements des Clusters nicht durch die Anwendung getroffen werden müssen, sondern durch das Cluster-Management vollkommen automatisch und transparent erfolgt.

Vor dem Hintergrund von Fig. 1 kann unser System wie folgt beschrieben werden. Anwendungsschlüssel (1) werden in Sicherheitselementen gehalten und dort sicher zur Anwendung gebracht (die in Fig. 1 dargestellte Verteilung der Schlüssel ist exemplarisch). Eine Vielzahl von einzelnen Sicherheitselementen (SE) (2) werden durch sogenannte Management Elemente (ME) (3) zu einem Verbund (Cluster) zusammengefasst. Zur sicheren (Um-)Verteilung der Anwendungsschlüssel innerhalb eines SE-Verbunds (das ist die Teilmenge unterhalb eines Management Elements) erfolgt durch das jeweilige Management Element. Ein Management Element stellt letztlich via Secure Channel die sicher End-to-End Übertragung von Anwendungsschlüsselmaterial zwischen ihm zugeordneten Sicherheitselementen sicher, ohne selbst Zugriff auf das Anwendungsschlüsselmaterial zu haben. Mehrere SE-Verbünde (4) sind an eine HKS Orchestrierung bzw. HKS-Management (5) angebunden. SE-Verbünde eines solchen Systems sind auch verteilt und standortübergreifend möglich. Eine derartige, mehrschichtige Elastizität des Systems ist daher gegeben, bleibt aber für Anwendungen transparent. Das HKS Management (5) bildet das Orchestrierungs- und Nutzungsverfahren ab und macht den SE-Verbund über Standard-APIs (6), wie zum Beispiel PKCS#11 oder anderen Schnittstellentechnologien, Anwendungen (7) nutzbar. Anwendungen bleibt die Komplexität des Systems somit verborgen.

Unser Verfahren zur elastischen Nutzung eines Verbunds (Cluster) von kryptographischen Sicherheitselementen für die performante Durchführung von kryptographischen Operationen würde eine kryptographische Operation beispielsweise wie folgt durchführen:

i. ein Verbund (Cluster) (2) aus kryptographischen Sicherheitselementen wird in einer elastischen Struktur organisiert;
ii. dieser Verbund wird mit kryptographischen Schlüsselmaterial (1) initialisiert, entweder durch das anwendungsseitige Einbringen von Schlüsselmaterial oder durch Generierung des Schlüsselmaterials in den kryptographischen Sicherheitselementen;

iii. das Schlüsselmaterial wird in Abhängigkeit der Sicherheitseigenschaften des Schlüsselmaterials und der Performanceanforderungen auf eine entsprechende Anzahl von kryptographischen Sicherheitselementen übertragen;

iv. die anwendungsseitigen, kryptographischen Einzeloperationen werden an die im vorherigen Schritt mit dem betreffenden Schlüsselmaterial vorbereiteten, kryptographischen Sicherheitselemente des Verbundes (5) zur Durchführung delegiert;

v. die Ergebnisse der parallelen Einzeloperationen werden als Ergebnis der anfordernden Anwendung (7) retourniert;

vi. das Verfahren (HKS-Management (5)) reorganisiert nach Abschluss einer kryptographischen Operation die Schlüsselverteilung erneut und bereitet den Verbund von Sicherheitselemente für neue anwendungsseitige Operationen vor;

vii. das Verfahren verwaltet die Sicherheitselemente dynamisch und verfolgt und steuert parallel zur Abwicklung von kryptographischen Operationen auch die Lebensdauer und Nutzbarkeit der einzelnen Sicherheitselemente.

Die Sicherheit des Gesamtverfahren wird vordergründig durch die verwendeten kryptographischen Sicherheitselemente begründet und das Verfahren selbst dient primär zur Orchestrierung des Verbunds an Sicherheitselementen.

Hauptanspruch

(1) Verfahren zur Nutzung eines Verbunds (Cluster) von kryptographischen Sicherheitselementen dadurch gekennzeichnet, dass für die performante Durchführung von kryptographischen Operationen ein Verbund (Cluster) aus kryptographischen Sicherheitselementen elastisch genutzt werden, indem auf deren Einzelelemente die erforderlichen kryptographischen Einzeloperationen agil verteilt werden.

Unteransprüche

(2) Verfahren nach Anspruch (1) dadurch gekennzeichnet, dass die einzelnen Sicherheitselemente im Verbund anforderungselastisch orchestriert werden.

(3) Verfahren nach einem der Ansprüche (1) bis (2) dadurch gekennzeichnet, dass die Sicherheitselemente in einer Baumstruktur organisiert sind.

(4) Verfahren nach einem der Ansprüche (1) bis (3) dadurch gekennzeichnet, dass das Verfahren dynamisch um eine beliebige Anzahl von Sicherheitselementen erweitert werden kann.

(5) Verfahren nach einem der Ansprüche (1) bis (4) dadurch gekennzeichnet, dass dieser Verbund mit kryptographischen Schlüsselmaterial initialisiert wird, entweder durch das anwendungsseitige Einbringen von Schlüsselmaterial oder durch Generierung des Schlüsselmaterials in den kryptographischen Sicherheitselementen.

(6) Verfahren nach einem der Ansprüche (1) bis (5) dadurch gekennzeichnet, dass das kryptographische Schlüsselmaterial nach dessen Einbringung bzw. Generation ausschließlich in kryptographischen Sicherheitselementen gehalten wird.

(7) Verfahren nach einem der Ansprüche (1) bis (6) dadurch gekennzeichnet, dass eine definierbare Anzahl von Sicherheitselementen ausschließlich zur Verwaltung von Schlüsselmaterial genutzt wird.

(8) Verfahren nach einem der Ansprüche (1) bis (7) dadurch gekennzeichnet, dass das Schlüsselmaterial in Abhängigkeit der Sicherheitseigenschaften des Schlüsselmaterials und/oder in Abhängigkeit der Performance-Anforderungen an die kryptographischen Operationen auf eine entsprechende Anzahl von kryptographischen Sicherheitselementen verteilt wird.

(9) Verfahren nach einem der Ansprüche (1) bis (8) dadurch gekennzeichnet, dass durch eine geeignete Initial-Parametrisierung, die der Abwägung zwischen Performance und Lebensdauer

folgt, eine entsprechend geeignete Orchestrierungsstrategie des HKS-Managements ausgewählt werden kann (Dispositionsschema).

(10) Verfahren nach einem der Ansprüche (1) bis (9) dadurch gekennzeichnet, dass die Disposition einzelner kryptographischer Sicherheitselemente nach einem definierbaren Dispositionsschema (Initial-Parametrisierung) erfolgt, um für eine langfristige Nutzung eine Anzahl an Sicherheitselementen als Betriebsreserve zu halten.

(11) Verfahren nach einem der Ansprüche (1) bis (10) dadurch gekennzeichnet, dass die Lebensdauer und die Verfügbarkeit einzelner Sicherheitselemente des Verbundes durch Messung deren Fehlerarte und Anzahl von bereits durchgeführten Operationen (Lese/Schreib-Zyklen) bestimmt und einzelne Elemente dementsprechend gezielt in oder außer Betrieb nimmt.

(12) Verfahren nach einem der Ansprüche (1) bis (11) dadurch gekennzeichnet, dass die Umverteilung von Schlüsselmaterial zwischen den Elementen eines Verbunds nur im Wege sicherer Ende-zu-Ende Verschlüsselung durchgeführt werden kann.

(13) Verfahren nach einem der Ansprüche (1) bis (12) dadurch gekennzeichnet, dass die Management-Elemente des SE-Verbunds die sichere Übertragung von Schlüsselmaterial innerhalb der einem Management-Element zugeordneten Menge an Sicherheitselementen gewährleisten (Secure Channel).

(14) Verfahren nach einem der Ansprüche (1) bis (13) dadurch gekennzeichnet, dass die anwendungsseitigen, kryptographischen Einzeloperationen an die mit dem betreffenden Schlüsselmaterial vorbereiteten kryptographischen Sicherheitselemente zur Durchführung delegiert werden.

(15) Verfahren nach einem der Ansprüche (1) bis (14) dadurch gekennzeichnet, dass die Ergebnisse der parallelen Einzeloperationen als Ergebnis der anfordernden Anwendung retourniert werden.

(16) Verfahren nach einem der Ansprüche (1) bis (15) dadurch gekennzeichnet, dass nach Abschluss einer kryptographischen Operation die Schlüsselverteilung erneut reorganisiert und der Verbund von Sicherheitselemente für neue anwendungsseitige Operationen vorbereitet werden.

(17) Verfahren nach einem der Ansprüche (1) bis (16) dadurch gekennzeichnet, dass die Grundfunktionen der einzelnen kryptographischen Sicherheitselemente im Verfahren auch direkt für Anwendungen nutzbar sind.

(18) Verfahren nach einem der Ansprüche (1) bis (17) dadurch gekennzeichnet, dass bestehende Anwendungen und Funktionen (Fremdanwendungen, Applets, etc.) der kryptographischen Sicherheitselemente Anwendungen auch direkt zugänglich und nutzbar gemacht werden können.

(19) Verfahren nach einem der Ansprüche (1) bis (18) dadurch gekennzeichnet, dass das Orchestrierungsverfahren rekursiv auch auf den Verbund von Systemen, die nach diesem Verfahren implementiert wurden, angewendet werden kann, um die Elastizität auch auf einer höheren Systemabstraktionsebene umsetzen zu können.

Zeichnungen

Figur 1

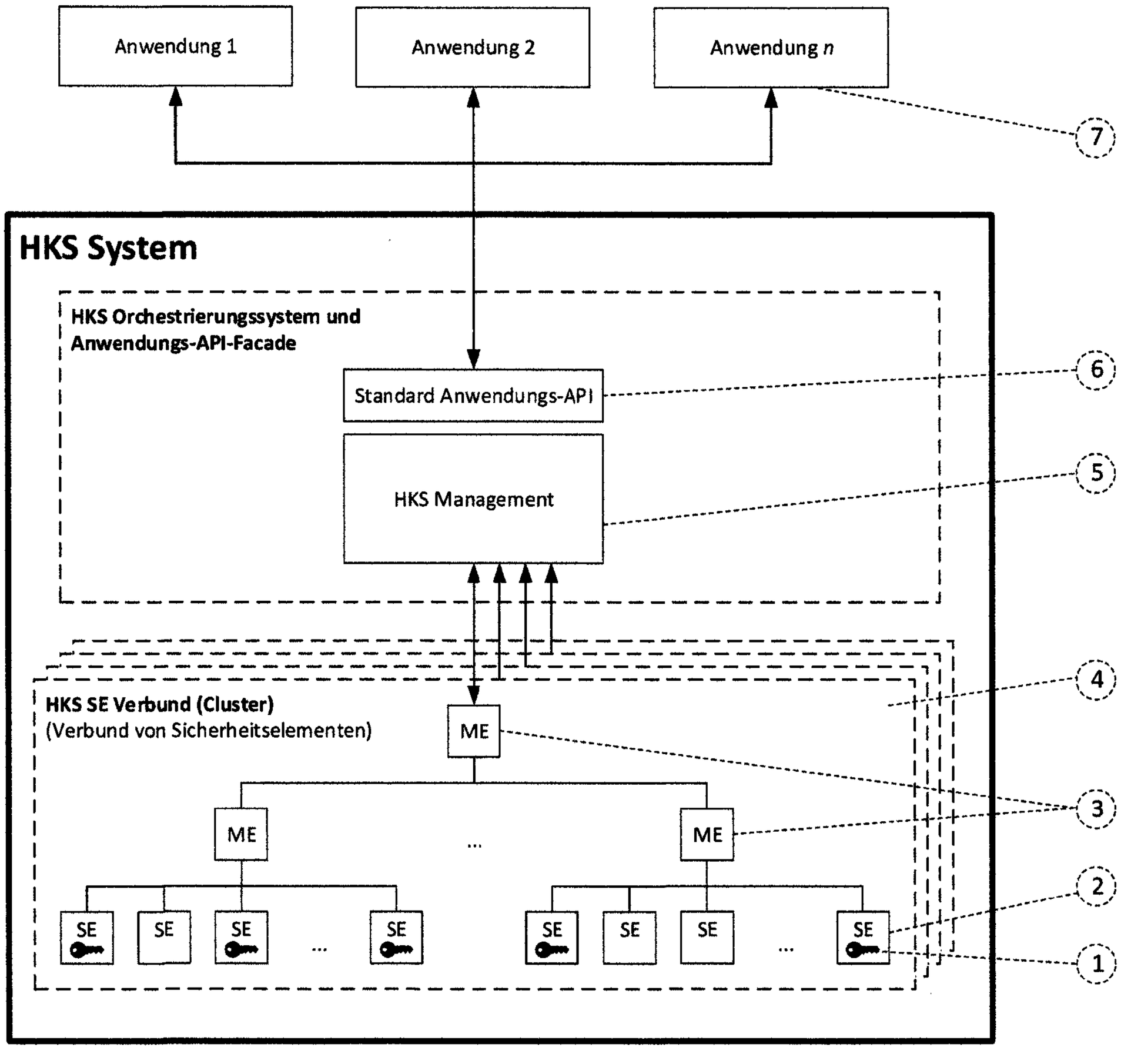

Fig. 1

Recherchenbericht zu **A 267/2019**

österreichisches patentamt

Klassifikation des Anmeldungsgegenstands gemäß IPC:
G06F 21/12 (2013.01); ***G06F 21/44*** (2013.01); ***G06F 21/45*** (2013.01); ***H04L 9/00*** (2006.01); ***H04L 9/08*** (2006.01)

Klassifikation des Anmeldungsgegenstands gemäß CPC:
G06F 21/123 (2013.01); ***G06F 21/44*** (2015.11); ***G06F 21/45*** (2015.11); ***H04L 9/00*** (2018.05); ***H04L 9/0836*** (2013.01)

Recherchierter Prüfstoff (Klassifikation):
G06F, H04L

Konsultierte Online-Datenbank:
WPIAP; EPODOC; TXTDE; TXTEN; INSPEC; NPL; Internet

Dieser Recherchenbericht wurde zu den am **02.08.2019** eingereichten Ansprüchen **1-19** erstellt.

Kategorie*)	Bezeichnung der Veröffentlichung: Ländercode, Veröffentlichungsnummer, Dokumentart (Anmelder), Veröffentlichungsdatum, Textstelle oder Figur soweit erforderlich	Betreffend Anspruch
X	US 2019080091 A1 (KIM KUN-YONG et al.) 14. März 2019 (14.03.2019) Siehe besonders Zusammenfassung; Fig. 1, 3 und die dazugehörigen Figurenbeschreibungen; Patentansprüche 1 bis 20	1-3
A		4-19
X	EP 3337119 A1 (NXP B.V.) 20. Juni 2018 (20.06.2018) Siehe besonders Zusammenfassung; Fig. 1, 5 und die dazugehörigen Figurenbeschreibungen; Paragraphen 1-5 und 129 bis 148; Patentansprüche 1 bis 14	1-2
A		3-19
X	WO 2018183926 A1 (UNIV NORTHERN ARIZONA) 04. Oktober 2018 (04.10.2018) Siehe besonders Zusammenfassung; Fig. 1, 4A, 4B und die dazugehörigen Figurenbeschreibungen; Paragraphen 1, 2, 12 und 13; Patentansprüche 1 bis 20	1
A		2-19
A	US 2018129801 A1 (CAMBOU BERTRAND FRANCIS) 10. Mai 2018 (10.05.2018) Siehe besonders Zusammenfassung; Fig. 2.0, 3.0 und die dazugehörigen Figurenbeschreibungen; Paragraphen 28-30 und 77; Patentansprüche 1 bis 20	1-19
A	PREETIDA VIANAYAKRAY-JANI et al. “Security Architecture for Cluster based Ad Hoc Networks” 06.07.2012; abgerufen im Internet am 10.06.2020 unter dem Link: <http://www.tifr.res.in/~sanyal/papers/Security_Architecture_for_Cluster_based_Ad_Hoc_Networks.pdf> Siehe Seiten 1 bis 5	1-19

Datum der Beendigung der Recherche:	Seite 1 von 1	Prüfer(in):
11.06.2020		KÖGL Christian

*) **Kategorien** der angeführten Dokumente:

X Veröffentlichung **von besonderer Bedeutung**: der Anmeldungsgegenstand kann allein aufgrund dieser Druckschrift nicht als neu bzw. auf erfinderischer Tätigkeit beruhend betrachtet werden.

Y Veröffentlichung **von Bedeutung**: der Anmeldungsgegenstand kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren weiteren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese **Verbindung für einen Fachmann naheliegend** ist.

A Veröffentlichung, die den allgemeinen **Stand der Technik** definiert.

P Dokument, das von **Bedeutung** ist (Kategorien **X** oder **Y**), jedoch **nach dem Prioritätstag** der Anmeldung veröffentlicht wurde.

E Dokument, das **von besonderer Bedeutung** ist (Kategorie **X**), aus dem ein „**älteres Recht**“ hervorgehen könnte (früheres Anmeldedatum, jedoch nachveröffentlicht, Schutz ist in Österreich möglich, würde Neuheit in Frage stellen).

& Veröffentlichung, die Mitglied der selben **Patentfamilie** ist.

Patentansprüche

1. Verfahren zur performanten Durchführung von kryptographischen Einzeloperationen, dadurch gekennzeichnet, dass
    a. eine Vielzahl von einzelnen kryptographischen Sicherheitselementen (2), durch Management-Elemente (3) zu einem Verbund (4) zusammengefasst werden, wobei
    b. dieser Verbund (4) mit kryptographischem Schlüsselmaterial (1) initialisiert wird, entweder
        i. durch das anwendungsseitige Einbringen von Schlüsselmaterial (1), oder
        ii. durch Generierung des Schlüsselmaterials (1) in den kryptographischen Sicherheitselementen (2), wobei
    c. das Schlüsselmaterial (1) in Abhängigkeit der Sicherheitseigenschaften des Schlüsselmaterials (1) und/oder der Performanceanforderungen an die kryptografischen Einzeloperationen auf eine entsprechende Anzahl von kryptographischen Sicherheitselementen (2) übertragen wird, wobei
    d. die kryptographischen Einzeloperationen an die kryptographischen Sicherheitselemente (2) des Verbunds (4) zur Durchführung delegiert werden, und
    e. die Ergebnisse der parallelen Einzeloperationen als Ergebnis der anfordernden Anwendung (7) retourniert werden.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass das kryptographische Schlüsselmaterial (1) nach dessen Einbringung bzw. Generierung ausschließlich in den kryptographischen Sicherheitselementen (2) gehalten wird.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass eine definierbare Anzahl von Sicherheitselementen (2) ausschließlich zur Verwaltung von Schlüsselmaterial (1) genutzt wird.

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass ein übergeordnetes HKS-Management (5) ein Orchestrierungs- und Nutzungsverfahren abbildet und den Verbund (4) über Standard-APIs (6) externen Anwendungen (7) nutzbar macht.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass die Disposition einzelner kryptographischer Sicherheitselemente (2) nach einem definierbaren Dispositionsschema (Initial-Parametrisierung) erfolgt, um für eine langfristige Nutzung eine Anzahl an Sicherheitselementen (2) als Betriebsreserve zu halten.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass die Lebensdauer und die Verfügbarkeit einzelner Sicherheitselemente (2) des Verbunds (4) durch Messung von deren Fehlerrate und Anzahl von bereits durchgeführten Operationen (Lese/Schreib-Zyklen) bestimmt wird, wobei einzelne Sicherheitselemente (2) gezielt in oder außer Betrieb genommen werden.

7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass die Umverteilung von Schlüsselmaterial (1) zwischen den Sicherheitselementen (2) eines Verbunds (4) nur im Wege sicherer Ende-zu-Ende Verschlüsselung durchgeführt wird.

8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass eine sichere End-to-End Übertragung von Schlüsselmaterial (1) innerhalb der einem Management-Element (3) zugeordneten Menge an Sicherheitselementen (2) durch die Management-Elemente (3) über Secure Channel erfolgt, ohne dass dabei die Management-Elemente (3) selbst Zugriff auf das Schlüsselmaterial (1) haben.

9. Verfahren nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, dass nach Abschluss einer kryptographischen Operation die Schlüsselverteilung erneut reorganisiert und der Verbund (4) von Sicherheitselementen (2) für neue anwendungsseitige Operationen vorbereitet wird.

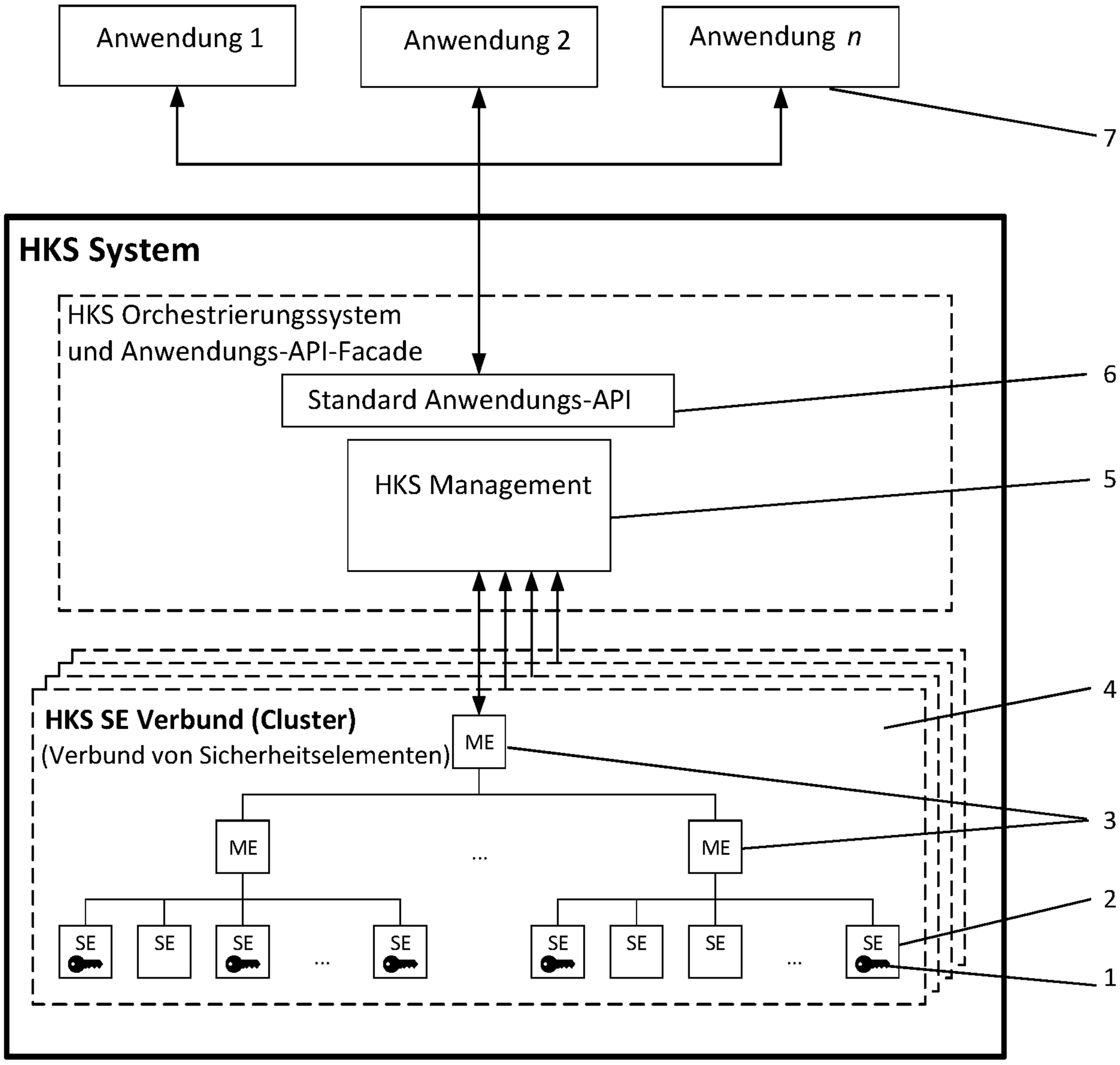

Fig. 1

ZULETZT VORGELEGTE ZEICHNUNGEN