(19) Deutsches Patent- und Markenamt

(10) **DE 11 2013 004 444 T5** 2015.07.30

(12) # Veröffentlichung

der internationalen Anmeldung mit der
(87) Veröffentlichungs-Nr.: **WO 2014/043040**
in deutscher Übersetzung (Art. III § 8 Abs. 2 IntPatÜG)
(21) Deutsches Aktenzeichen: **11 2013 004 444.7**
(86) PCT-Aktenzeichen: **PCT/US2013/058818**
(86) PCT-Anmeldetag: **09.09.2013**
(87) PCT-Veröffentlichungstag: **20.03.2014**
(43) Veröffentlichungstag der PCT Anmeldung
in deutscher Übersetzung: **30.07.2015**

(51) Int Cl.: ***H04W 12/08*** (2009.01)
H04W 88/02 (2009.01)

(30) Unionspriorität:

13/612,641	**12.09.2012**	**US**
61/704,405	**21.09.2012**	**US**

(71) Anmelder:
Apple Inc., Cupertino, Calif., US

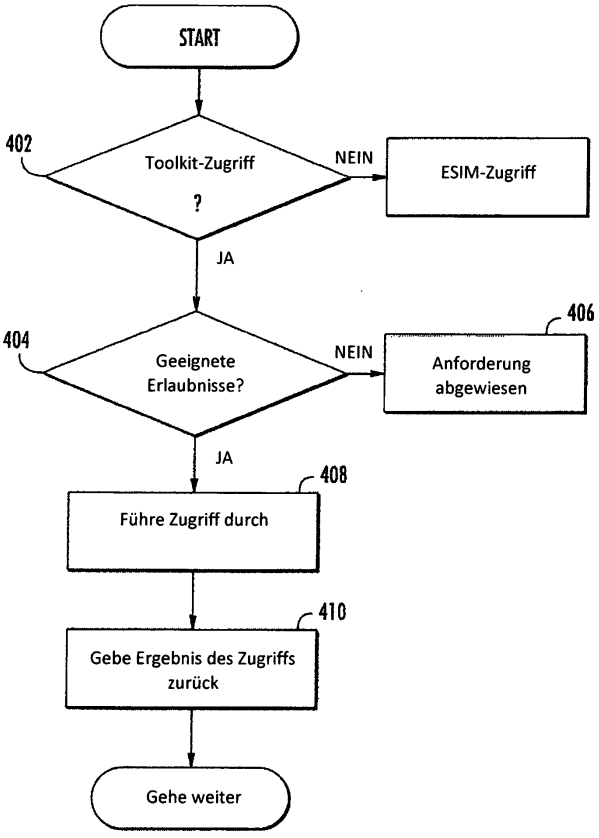
(74) Vertreter:
BARDEHLE PAGENBERG Partnerschaft mbB Patentanwälte, Rechtsanwälte, 81675 München, DE

(72) Erfinder:
Li, Li, Cupertino, Calif., US; Juang, Ben-Heng, Cupertino, Calif., US; Mathias, Arun G., Cupertino, Calif., US; Hauck, Jerrold von, Cupertino, Calif., US

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Verfahren und Vorrichtung zum Verwalten von Daten in einem sicheren Element**

(57) Zusammenfassung: Vorrichtung und Verfahren zum Verwalten und Teilen von Daten über mehrere Zugriffssteuerungsclienten in Vorrichtungen sind hierin offenbart. Bei einem Ausführungsbeispiel weisen die Zugriffssteuerungsclienten elektronische Subscriber Identity Module (eSIMs) auf, die auf einer eingebetteten Universal Integrated Circuit Card (eUICC) angeordnet sind. Jedes eSIM enthält seine eigenen Daten. Eine Advanced Subscriber Identity Toolkit-Anwendung, die in der eUICC gehalten wird, erleichtert das Verwalten und Teilen von Daten mehrerer eSIMs für verschiedene Zwecke wie z. B. Teilen von Telefonbuch-Kontakten oder Erleichtern des automatischen Umschaltens zwischen den mehreren eSIMs (wie z. B. basierend auf Benutzerkontext).



Beschreibung

Gebiet der Erfindung

[0001] Die vorliegende Erfindung bezieht sich allgemein auf das Gebiet der Kommunikationssysteme und insbesondere in einem beispielhaften Aspekt darauf, das Teilen von Daten zwischen mehreren Benutzerzugriffsclienten auf einer oder mehreren mobilen Vorrichtungen zu erleichtern.

Beschreibung der verwandten Technologie

[0002] Eine Zugriffssteuerung ist für die sichere Kommunikation in den meisten drahtlosen Funkkommunikationssystemen des Standes der Technik erforderlich. Beispielsweise kann ein einfaches Zugriffssteuerungsschema aufweisen: (i) Verifizieren der Identität einer kommunizierenden Partei, und (ii) Gewähren eines Zugriffsniveaus, das der verifizierten Identität entspricht. Im Kontext eines beispielhaften zellularen Systems (z. B. Universal Mobile Telecommunications System (UMTS)), wird die Zugriffssteuerung durch einen Zugriffssteuerungsclienten geregelt, der als ein Universal Subscriber Identity Module (USIM) bezeichnet wird, das auf einer physikalischen Universal Integrated Circuit Card (UICC) (auch als ”SIM-Karte” bezeichnet) abläuft. Der USIM-Zugriffssteuerungsclient authentifiziert den Teilnehmer gegenüber dem zellularen UMTS-Netzwerk. Nach einer erfolgreichen Authentifizierung wird dem Teilnehmer erlaubt, auf das zellulare Netzwerk zuzugreifen. Wie hiernach verwendet bezieht sich der Begriff ”Zugriffssteuerungsclient” im Allgemeinen auf eine logische Einheit, die entweder in Hardware oder Software oder Kombinationen davon ausgeführt ist, geeignet zum Steuern des Zugriffs einer ersten Vorrichtung auf ein Netzwerk. Bekannte Beispiele von Zugriffssteuerungsclienten umfassen das zuvor erwähnte USIM, CDMA Subscriber Identification Modul (CSIM), IP Multimedia Services Identity Modul (ISIM), Subscriber Identity Modul (SIM), Removable User Identity Modul (RUIM) usw. Traditionellerweise setzt die UICC eine vertrauenswürdige Grenze für einen oder mehrere USIM(oder allgemeiner ”SIM”) -Zugriffssteuerungsclienten. Die UICC wird hergestellt und ”fest codiert” mit einem SIM, d. h. einmal programmiert kann die UICC nicht neu programmiert werden. Wenn ein Benutzer sich bei einem zellularen Netzwerk unter Verwendung eines anderen SIM authentifizieren will, muss der Benutzer die SIM-Karte physisch in der Vorrichtung gegen eine unterschiedliche SIM-Karte austauschen. In Antwort auf diese physikalischen Beschränkungen sind einige Vorrichtungen entwickelt worden, die zwei SIM-Karten gleichzeitig aufzunehmen können, bekannt als Dual-SIM-Telefone. Dual-SIM-Telefone adressieren jedoch nicht die fundamentalen physikalischen Beschränkungen von SIM-Kartenvorrichtungen. Beispielsweise kann die Information, die innerhalb einer SIM-Karte gespeichert ist, nicht einfach mit Information zusammengeführt werden, die innerhalb einer anderen SIM-Karte gespeichert ist. Existierende Dual-SIM-Vorrichtungen können nicht auf die Inhalte beider SIM-Karten gleichzeitig zugreifen. Schließlich erfordert das Zugreifen auf eine SIM-Karte eine merkliche und nicht triviale Zeitdauer für den Benutzer; das Wechseln zwischen SIM-Karten, um Information zu übertragen, ist unerwünscht und reduziert das Benutzererlebnis und diese Einschränkung liegt sowohl bei traditionellen als auch Dual-SIM-Vorrichtungen vor.

[0003] Demgemäß werden neue Lösungen benötigt, um die Flexibilität beim Zugreifen auf mehrere Zugriffssteuerungsclienten zu erhöhen. Idealerweise sollten solche Lösungen das Teilen gemeinsamer Benutzerdaten zwischen den mehreren Zugriffssteuerungsclienten erlauben, um das Erlebnis des Benutzers zu verbessern. Außerdem sollten die verbesserten Verfahren und Vorrichtungen ein nahtloses Umschalten zwischen den mehreren Zugriffssteuerungsclienten erlauben, um den Zugriff eines Benutzers und die Benutzung von zellularen Diensten zu verbessern.

Zusammenfassung der beschriebenen Ausführungsbeispiele

[0004] Die vorliegende Erfindung befriedigt die oben genannten Wünsche durch Bereitstellen unter anderem einer verbesserten Vorrichtung und eines Verfahrens zum Teilen von Daten zwischen mehreren Benutzerzugriffsclienten einer oder mehrerer mobilen Vorrichtungen.

[0005] In einem Aspekt der vorliegenden Erfindung ist ein sicheres Element offenbart, das konfiguriert ist, um einen oder mehrere Zugriffssteuerungsclienten zu speichern, wobei jeder der einen oder mehreren Zugriffssteuerungsclienten Daten enthält. In einem Ausführungsbeispiel umfasst das sichere Element einen sicheren Prozessor und eine sichere Speichervorrichtung bei der Datenkommunikation mit dem sicheren Prozessor. In einer beispielhaften Ausführungsform umfasst die Speichervorrichtung computerausführbare Anweisungen, die konfiguriert sind, um, wenn sie durch den sicheren Prozessor ausgeführt werden, eine Anforderung zu empfangen, auf erste Daten eines inaktiven ersten Zugriffssteuerungsclienten zuzugreifen, die Anforderung zu verifizieren, auf die ersten Daten des inaktiven ersten Zugriffssteuerungsclienten zuzugreifen und die ersten Daten zurückzugeben.

[0006] Bei einer Variante umfasst jeder des einen oder der mehreren Zugriffssteuerungsclienten computerausführbare Anweisungen, die konfiguriert sind, um, wenn sie durch den sicheren Prozessor ausgeführt werden: eine Anforderung zu empfangen, einen aktiven zweiten Zugriffssteuerungsclienten von einer

Netzwerkeinheit zu authentifizieren; die Anforderung zu authentifizieren; und wenn die Anforderung authentisch ist, der Netzwerkeinheit zu antworten.

[0007] Bei einer anderen Variante haben Anforderungen, auf Daten zuzugreifen, und vom Netzwerk stammende Anforderungen unterschiedliche Privilegniveaus.

[0008] Bei einigen Varianten identifiziert die Anforderung einen Anforderer. Beispielsweise kann der Anforderer ein Benutzer sein. Bei einem anderen Beispiel kann der Anforderer eine Softwareanwendung sein. In solch einem Fall residiert die Softwareanwendung auf dem sicheren Element. Bei noch anderen Beispielen umfasst der Anforderer einen Softwareprozess auf einem zweiten des einen oder der mehreren Zugriffssteuerungsclienten auf dem sicheren Element.

[0009] Bei einem zweiten Aspekt ist ein Verfahren zum Verarbeiten von Daten innerhalb eines sicheren Elements offenbart, das konfiguriert ist, um einen oder mehrere Zugriffssteuerungsclienten zu speichern, von denen jeder Daten enthält. Bei einem Ausführungsbeispiel umfasst das Verfahren: Empfangen einer Anforderung, auf erste Daten zuzugreifen; Verifizieren der Anforderung; Suchen einer Vielzahl von Zugriffssteuerungsclienten für die ersten Daten; und wenn die ersten Daten gefunden wurden, Zurückgeben der ersten Daten.

[0010] Bei einer solchen Variante umfasst das Verifizieren der Anforderung das Identifizieren des Anforderers. Bei einem solchen Beispiel umfasst das Verifizieren der Anforderung weiter Bestimmen eines Privilegs, das dem Anforderer zugeordnet ist. Bei einem anderen Beispiel wird das bestimmte Privileg, das dem Anforderer zugeordnet ist, durch eine administrative Einheit vorbestimmt.

[0011] Bei anderen Varianten umfasst das Zugreifen auf die ersten Daten das Zugreifen auf eine Vielzahl von Kontaktinformationen, um einen einzelnen Kontakt zu identifizieren.

[0012] Bei noch anderen Varianten umfasst das Zugreifen auf die ersten Daten das Zugreifen auf eine oder mehrere Vorrichtungskonfigurationen, die Zugriffsfreigabekonfiguration einer Vorrichtung gemäß zumindest einer der einen oder mehreren Konfigurationen.

[0013] Bei einem dritten Aspekt ist ein sicheres Element offenbart, das konfiguriert ist, um einen oder mehrere Zugriffssteuerungsclienten zu speichern, wobei jeder der einen oder mehreren Zugriffssteuerungsclienten Daten enthält. In einem Ausführungsbeispiel umfasst das sichere Element: Mittel zum Empfangen einer Anforderung, um auf erste Daten zuzugreifen; Mittel, um die Anforderung zu verifizieren; Mittel zum Durchsuchen des einen oder der mehreren Zugriffssteuerungsclienten nach den ersten Daten; und Mittel zum Zurückgeben der ersten Daten.

[0014] Bei einer Variante weisen die Mittel zum Verifizieren der Anforderung Mittel zum Verifizieren einer persönlichen Identifizierungsnummer (PIN) oder eines Passwortes auf, das von einem Benutzer geliefert wird.

[0015] Bei anderen Varianten weisen die Mittel zum Verifizieren der Anforderung Mittel zum Bestimmen eines Softwareprivilegniveaus einer Softwareanwendung auf.

[0016] Bei noch anderen Varianten umfasst das sichere Element Mittel zum Empfangen einer Netzwerkanforderung, um den Zugriffssteuerungsclienten zu authentifizieren.

[0017] Bei einem vierten Aspekt ist eine mobile Vorrichtung offenbart. In einem Ausführungsbeispiel umfasst die mobile Vorrichtung: ein sicheres Element, wobei das sichere Element konfiguriert ist, um einen oder mehrere Zugriffssteuerungsclienten zu speichern, wobei jeder des einen oder der mehreren Zugriffssteuerungsclienten Daten enthält; eine oder mehrere drahtlose Kommunikationsschaltungen, die dazu geeignet sind, mit einem Kommunikationsnetzwerk zu kommunizieren; einen ersten Prozessor; eine Speichervorrichtung, die in Datenkommunikation mit dem ersten Prozessor ist, wobei die Speichervorrichtung computerausführbare Anweisungen enthält, die konfiguriert sind, um, wenn sie durch den ersten Prozessor ausgeführt werden, eine Anforderung zu übertragen, auf erste Daten eines ersten Zugriffssteuerungsclienten gemäß einem ersten Privileg zuzugreifen, wobei das erste Privileg auf Daten beschränkt ist, auf die durch ein Toolkit zugegriffen werden kann; wobei die Anforderung konfiguriert ist, um zu veranlassen, dass das sichere Element: die Anforderung verifiziert; auf die ersten Daten des ersten Zugriffssteuerungsclienten zugreift; und die ersten Daten zu dem ersten Prozessor zurückgibt.

[0018] In einem fünften Aspekt der vorliegenden Erfindung ist ein Verfahren zum Zugreifen auf Daten innerhalb eines sicheren Elementes einer Benutzervorrichtung offenbart. In einem Ausführungsbeispiel umfasst das Verfahren: Übertragen einer Anforderung, auf erste Daten zuzugreifen, die auf dem sicheren Element der Benutzervorrichtung gespeichert sind; in Antwort auf das Empfangen der Anforderung, Verifizieren das sichere Element der Anforderung durch das sichere Element; wenn die Anforderung gültig ist, Lokalisieren der ersten Daten auf einem der Vielzahl von Zugriffssteuerungsclienten; und Empfangen der ersten Daten von dem sicheren Element.

[0019] In einem sechsten Aspekt der vorliegenden Erfindung ist eine mobile Vorrichtung offenbart. In einem Ausführungsbeispiel umfasst die mobile Vorrichtung: ein sicheres Element, wobei das sichere Element konfiguriert ist, um einen oder mehrere Zugriffssteuerungsclienten zu speichern, wobei jeder der einen oder der mehreren Zugriffssteuerungsclienten Daten enthält; eine oder mehrere drahtlose Kommunikationsschaltungen, die dazu geeignet sind, mit einem Kommunikationsnetzwerk zu kommunizieren; Logik, die konfiguriert ist, um Zugriff auf erste Daten eines ersten der einen oder mehreren inaktiven Zugriffssteuerungsclienten anzufordern, die auf dem sicheren Element gespeichert sind; wobei das sichere Element konfiguriert ist, um die Anforderung zu verifizieren, und wenn die Anforderung gültig ist, die ersten Daten dem ersten Zugriffssteuerungsclienten bereitzustellen; und eine Logik, die konfiguriert ist, um die ersten Daten von dem sicheren Element zu empfangen.

[0020] Andere Merkmale und Vorteile der vorliegenden Erfindung werden unmittelbar von Fachleuten mit Bezug auf die beigefügten Zeichnungen und die detaillierte Beschreibung von beispielhaften Ausführungsformen wie unten angegeben erkannt werden.

Kurze Beschreibung der Zeichnungen

[0021] Fig. 1 veranschaulicht grafisch ein Beispiel eines Authentication and Key Agreement- (AKA)-Verfahrens, das ein USIM gemäß dem Stand der Technik benutzt.

[0022] Fig. 2 ist ein Blockdiagramm einer beispielhaften Ausführungsform einer Vorrichtung, die nützlich für die Implementierung der Verfahren der vorliegenden Erfindung ist.

[0023] Fig. 3 ist eine logische Darstellung einer beispielhaften Ausführungsform einer eingebetteten Universal Integrated Circuit Card (UICC) gemäß verschiedenen Aspekten der vorliegenden Erfindung.

[0024] Fig. 4 ist ein logisches Flussdiagramm eines Ausführungsbeispiels eines verallgemeinerten Verfahrens für die Verwaltung von Daten in einem sicheren Element gemäß verschiedenen Aspekten der vorliegenden Erfindung.

[0025] Fig. 5 ist ein logisches Flussdiagramm eines Ausführungsbeispiels eines Verfahrens zum Zusammenführen von benutzerdefinierten Kontaktinformationen mehrerer elektronischer Subscriber Identity Module (eSIMs) gemäß der vorliegenden Erfindung.

[0026] Fig. 6 ist ein logisches Flussdiagramm, das ein Ausführungsbeispiel eines Verfahrens zum Suchen nach Kontaktinformation in mehreren elektronischen Subscriber Identity Modulen (eSIMs) gemäß der vorliegenden Erfindung veranschaulicht.

[0027] Fig. 7 ist ein logisches Flussdiagramm, das ein Ausführungsbeispiel eines Verfahrens zum Erleichtern des automatischen Umschaltens zwischen elektronischen Subscriber Identity Moduls (eSIMs) basierend auf einer benutzerdefinierten bedingten Triggerung gemäß der vorliegenden Erfindung veranschaulicht.

Detaillierte Beschreibung der beschriebenen Ausführungsbeispiele

[0028] Es wird nun Bezug genommen auf die Zeichnungen, worin sich gleiche Bezugszeichen durchgehend auf gleiche Teile beziehen.

[0029] Die vorliegende Erfindung stellt unter anderem Verfahren und Vorrichtungen zum Verwalten und Teilen von Daten über zahlreiche Benutzerzugriffssteuerungsclienten in Vorrichtungen bereit. In einem Ausführungsbeispiel verwaltet eine eingebettete Universal Integrated Circuit Card (eUICC), ein sicheres Element oder eine UICC, die eine logische Einheit enthält (z. B. ein Advanced Subscriber Identity Toolkit) Daten und stellt Zugriff auf sie bereit, die über mehrere elektronische Subscriber Identity Module (eSIMs) gespeichert sind. Daten können beispielsweise aus benutzerdefinierten Daten (UDD), z. B. Einstellungen und Daten, die durch einen Nutzer konfiguriert worden sind, wie z. B. Telefonbuch-Kontakte, eSIM-Benutzer-Präferenzen usw.), Operator spezifischen Daten, Kalibrierungsdaten usw. bestehen. Das Advanced Subscriber Identity Toolkit stellt eine sekundäre privilegierte Schnittstelle bereit, die schnelleren Zugriff auf Daten ermöglicht, die in dem eSIM gespeichert sind, ohne die Integrität der eSIM-Sicherheit zu kompromittieren.

[0030] Noch andere Aspekte der vorliegenden Erfindung ermöglichen einen gemeinschaftlichen Betrieb von Zugriffssteuerungsclienten. Beispielsweise ist in einem beispielhaften Benutzungsfall eine logische Einheit wie z. B. die zuvor genannte Advanced Subscriber Identity Toolkit konfiguriert, um operationale oder andere Bedingungen einer Vorrichtung zu überwachen und sie gegenüber eSIM-Benutzungspräferenzen zu vergleichen, die durch einen Benutzer spezifiziert worden sind (oder, z. B. einen Netzwerkbetreiber, usw.). Die beispielhafte Implementierung des Advanced Subscriber Identity Toolkits kann außerdem automatisch die aktive eSIM gemäß den gewünschten Präferenzen umschalten.

[0031] Beispielhafte Ausführungsformen und Aspekte der vorliegenden Erfindung werden nun im Detail beschrieben werden. Während diese Ausführungsbeispiele und Aspekte primär im Kontext von Subscriber Identity Modulen (SIMs) eines GSM, GPRS/

EDGE, oder UMTS zellularen Netzwerks diskutiert werden, wird vom Fachmann erkannt werden, dass die vorliegende Erfindung nicht darauf beschränkt ist. Tatsächlich sind verschiedene Aspekte der Erfindung in jedem drahtlosen Netzwerk nützlich (ob zellular oder anders), das von der sicheren Verwaltung von mehreren Benutzerzugriffssteuerungsclienten profitieren kann.

[0032] Es wird auch erkannt werden, dass, während der Begriff "Subscriber Identity Module" hier verwendet wird (z. B. SIM, USIM, CSIM, eSIM usw.), dieser Begriff keineswegs notwendigerweise entweder (i) die Benutzung durch einen Teilnehmer per se (d. h. die Erfindung kann durch einen Teilnehmer oder Nicht-Teilnehmer praktiziert werden); (ii) die Identität eines einzelnen Individuums (d. h. die Erfindung kann von einer Gruppe von Individuen, wie z. B. einer Familie, oder nicht greifbaren oder fiktiven Einheiten wie z. B. einem Unternehmen benutzt werden); oder (iii) irgendeine greifbare "Modul"-Ausrüstung oder Hardware, beinhaltet oder erfordert.

Subscriber Identity Module(SIM)-Betrieb

[0033] Im Kontext von zellularen UMTS-Netzwerken des Standes der Technik umfasst ein Benutzergerät (UE) eine mobile Vorrichtung und ein Universal Subscriber Identity Modul (USIM). Das USIM ist eine logische Softwareeinheit, die auf einer physikalischen Universal Integrated Circuit Card (UICC) gespeichert ist und von ihr ausgeführt wird. Eine Vielzahl von Informationen sind in dem USIM gespeichert, wie z. B. Teilnehmerinformation sowie auch die Schlüssel und Algorithmen, die zur Authentifizierung mit dem Netzwerkbetreiber benutzt werden, um die drahtlosen Netzwerkdienste zu erhalten. Bei einigen alternativen Implementierungen sind die Schlüssel und/oder kryptografischen Algorithmen in dem Betriebssystem der UICC gespeichert. Die USIM-Software basiert auf der Java Card Programmiersprache. Java Card ist eine Untermenge der Java-Programmiersprache, die für eingebettete Vorrichtungen vom "Karten"-Typ modifiziert worden ist (wie z. B. die zuvor genannte UICC).

[0034] Im Allgemeinen sind UICCs mit einem USIM vor der Verteilung an den Teilnehmer programmiert. Das Vorprogrammieren oder "Personalisieren" ist spezifisch für jeden Netzwerkbetreiber. Beispielsweise ist dem USIM vor der Verwendung eine International Mobile Subscriber Identify (IMSI), ein einzigartiger Integrated Circuit Card Identifier (ICCID) und ein spezifischer Authentifizierungsschlüssel (K) zugeordnet. Der Netzwerkbetreiber speichert die Zuordnung in einem Register, das in dem Authentifizierungszentrum (AuC) des Netzwerks enthalten ist. Nach dem Personalisieren kann die UICC an die Teilnehmer verteilt werden. Nun Bezug nehmend auf die **Fig.** 1 ist ein beispielhaftes Authentification and Key Agreement(AKA)-Verfahren im Detail veranschaulicht, das das zuvor genannte USIM des Standes der Technik benutzt. Während normalen Authentifizierungsverfahren erhält das UE die International Mobile Subscriber Identify (IMSI) von dem USIM. Das UE gibt die IMSI an das bedienende Netzwerk (SN) des Netzwerkbetreibers oder das besuchte Kernnetzwerk weiter. Das SN gibt die Authentifizierungsanforderung an das AuC des Heimnetzwerkes (HN) weiter. Das HN vergleicht die empfangene IMSI mit dem Register des AuC und erhält den geeigneten Schlüssel K. Das HN erzeugt eine zufällige Zahl (RAND) und unterzeichnet sie mit dem Schlüssel K unter Verwendung eines Algorithmus, um die erwartete Antwort (XRES) zu erzeugen. Das HN erzeugt weiter einen Cipher Key (CK) und einen Integrity Key (IK) zur Benutzung bei dem Chiffrier- und Integritätsschutz ebenso wie ein Authentication Token (AUTN), der verschiedene Algorithmen benutzt. Das HN sendet einen Authentifizierungsvektor, der aus den RAND, XRES, CK und AUTN besteht, an das SN. Das SN speichert den Authentifizierungsvektor nur zur Benutzung in einem einmaligen Authentifizierungsprozess. Das SN gibt das RAND und AUTN an das UE.

[0035] Wenn das UE die RAND und AUTN empfängt, verifiziert die USIM, ob die empfangene AUTN gültig ist. Wenn dies so ist, benutzt das UE die empfangene RAND, um seine eigene Antwort zu berechnen (RES) unter Verwendung des gespeicherten Schlüssels K und des gleichen Algorithmus, der die XRES generiert hat. Das UE gibt die RES zurück zu dem SN. Das SN vergleicht die XRES mit der empfangenen RES und, wenn sie zusammenpassen, autorisiert das SN das UE, die Drahtlosnetzwerkdienste des Betreibers zu benutzen.

[0036] Zusätzlich dazu, dass die UICC mit einem USIM programmiert ist, ist die UICC im Allgemeinen mit anderen Anwendungen programmiert, die eine verbesserte Funktionalität für die UICC bereitstellen. Allgemeine Beispiele solcher Anwendungen sind ein Telefonbuch oder ein USIM Application Toolkit (USAT). Das USAT wird typischerweise als eine Value Added Service-Technologie verwendet, die das Kommunikationsprotokoll zwischen der UICC und der Vorrichtung erweitert.

Verschlüsselung/Schlüsselschemata

[0037] Asymmetrische Schlüsselschemata verwenden unterschiedliche Schlüssel, um Nachrichten zu verschlüsseln und zu entschlüsseln, und daher teilen sich der Verschlüsseler und der Entschlüsseler nicht denselben Schlüssel. Symmetrische Schlüsselschemata verwenden denselben Schlüssel (oder trivial transformierte Schlüssel) sowohl zum Verschlüsseln als auch zum Entschlüsseln. Der Rivest, Shamir und Adleman-(RSA)-Algorithmus ist ein Typ von öffentlicher/privater Schlüsselpaarkryptografie, der all-

gemein im Stand der Technik benutzt wird, aber es wird erkannt werden, dass die vorliegende Erfindung keineswegs auf den RSA-Algorithmus beschränkt ist. Öffentliche/private Kryptografieschemata können verwendet werden, um eine Nachricht zu verschlüsseln und/oder Signaturen zu erzeugen. Spezifisch kann eine Nachricht mit einem privaten Schlüssel verschlüsselt werden und mit einem öffentlichen Schlüssel entschlüsselt werden, wodurch gewährleistet wird, dass die Nachricht nicht beim Übergang verändert worden ist. Ähnlich kann eine Signatur, die mit dem privaten Schlüssel erzeugt worden ist, mit dem öffentlichen Schlüssel verifiziert werden, was gewährleistet, dass die Einheit, die die Signatur erzeugt, legitimiert ist. Bei beiden Benutzungen wird der private Schlüssel versteckt gehalten und der öffentliche Schlüssel wird frei verteilt.

Gerät

[0038] Als eine kurze Randbemerkung können die UICCs des Standes der Technik (z. B. eine SIM-Karte) frei zwischen mobilen Vorrichtungen bewegt werden, aber das SIM selbst ist in der UICC fest codiert. Während SIM-Karten mit vielfachen SIMs vorprogrammiert werden können (z. B. ein USIM und ein CSIM usw.), enthalten die bestehenden Entwicklungen allgemein nur ein einzelnes SIM. Gemäß bestehenden SIM-Vertrauensarchitekturen ist die mobile Vorrichtung keine vertrauenswürdige Einheit; daher muss die SIM-Karte bestimmen, ob die mobile Vorrichtung kompromittiert worden ist, bevor Zugriff gewährt wird. Tatsächlich ist die SIM nur konfiguriert, um vertrauliche Kommunikationen mit einem Heimnetzwerk (HN) oder einem Serving Netzwerk (SN) aufzubauen, das Zugriff auf geeignete kryptografische Geheimnisse hat.

[0039] Zusätzlich gibt es keinen Mechanismus bei bestehenden Lösungen zum Authentifizieren einer SIM-Karte zu einer anderen SIM-Karte, daher ist die ”Vertrauensgrenze” jeder SIM-Karte auf die Karte selbst beschränkt. Teilen von Information zwischen SIM-Karten erfordert, dass eine mobile Vorrichtung sicher auf jede SIM-Karte zugreifen kann und extern Information zwischen SIM-Karten transferiert.

[0040] Im Gegensatz dazu ist gemäß einem Aspekt der vorliegenden Erfindung ein sicheres Element (UICC, eUICC usw.) konfiguriert, um vielfache SIM-Elemente zu speichern, die hiernach als Electronic Subscriber Identity Modules (eSIM) bezeichnet werden. Jedes eSIM ist eine Softwareemulation eines typischen USIM, und enthält analoges Programmieren und damit verbundene Benutzerdaten. Bei einigen Varianten kann ein eSIM zusätzliche Software und/oder Anwendungen zusätzlich zu den USIM-Anwendungen umfassen. Bei einer beispielhaften Ausführungsform ist eine eingebettete UICC (eUICC), die in einer mobilen Vorrichtung residiert, zur Benutzung mit einer Advanced Subscriber Identity Toolkit-Softwareschicht konfiguriert, um die vielfachen eSIMs zu verwalten und darauf zuzugreifen, die darauf gespeichert sind. Verschiedene Ausführungsbeispiele der vorliegenden Erfindung haben eine permanent montierte eUICC-Komponente, die nicht ohne große Anstrengung von der mobilen Vorrichtung entfernt werden kann. Außerdem, während die eUICC noch eine Vertrauensgrenze mit der mobilen Vorrichtung durchsetzt, sind die vielfachen eSIMs intern innerhalb der eUICC-Vertrauensgrenze gespeichert und können sicher innerhalb der eUICC-Vertrauensgrenze modifiziert und/oder manipuliert werden.

[0041] Bezug nehmend jetzt auf die **Fig.** 2 ist eine beispielhafte Ausführungsform einer Vorrichtung **200** veranschaulicht, die nützlich zum Implementieren der Verfahren der vorliegenden Erfindung ist. Die beispielhafte Vorrichtung **200** umfasst einen Anwendungsprozessor **202**, ein sicheres Element **204** und eine oder mehrere drahtlose Schnittstellen und zugeordnete Baseband-Prozessoren **206**. Obwohl als UMTS-konformes Benutzergerät (UE) eine mobile drahtlose Vorrichtung gezeigt ist, wird begrüßt werden, dass die Vorrichtung **200** praktisch jeden Formfaktor oder Merkmale annehmen kann, die mit der Erfindung konsistent sind.

[0042] Wie gezeigt umfasst der Anwendungsprozessor **202** einen digitalen Signalprozessor, Mikroprozessor, feldprogrammierbares Gate-Array oder eine Vielzahl von verarbeitenden Komponenten, die auf ein oder mehrere Substrate montiert sind. Das verarbeitende Untersystem kann auch einen internen Cache-Speicher umfassen. Das verarbeitende Untersystem ist mit einem Speicher-Untersystem verbunden, das einen Speicher aufweist, der beispielweise SRAM-, Flash- und SDRAM-Komponenten aufweisen kann. Das Speicher-Untersystem kann eine oder mehrere Hardware vom DMA-Typ implementieren, um Datenzugriffe zu erleichtern, wie es im Stand der Technik wohl bekannt ist. Das Speicher-Untersystem enthält computerausführbare Anweisungen, die durch das Prozessor-Untersystem ausführbar sind.

[0043] Das sichere Element **204** umfasst einen sicheren Prozessor (z. B. einen sicheren Mikroprozessor des Typs, der in der digitalen Verarbeitungstechnik bekannt ist) und zugeordneten sicheren Speicher. Der sichere Speicher enthält computerausführbare Anweisungen, die durch den sicheren Prozessor ausführbar sind. Anders als die anderen Prozessoren der Vorrichtung ist das sichere Element von anderer Software isoliert; insbesondere ist das sichere Element permanent oder semi-permanent konfiguriert, um eine Codebasis auszuführen, von der bekannt ist, dass sie sicher ist. Bei einigen Varianten kann die sichere Codebasis nicht modifiziert werden. Bei anderen Varianten kann die sichere Codebasis nur unter strikten Bedingungen modifiziert werden (z. B. eine Ver-

bindung zu einer vertrauenswürdigen Partei, wie z. B. dem Hersteller, usw.).

[0044] Das sichere Element umfasst eine virtuelle oder elektronische Einheit, wie z. B. eine Softwareanwendung, die hiernach als eine Embedded Universal Integrated Circuit Card (eUICC) bezeichnet wird. Bei einer solchen Variante ist die eUICC in der Lage, vielfache eSIMs zu speichern und zu verwalten. Die eUICC wählt ein eSIM basierend auf der ICCID des eSIM aus. Wenn die eUICC das gewünschte (n) eSIM(s) auswählt, kann das UE ein Authentifizierungsverfahren initiieren, um drahtlose Netzwerkdienste von dem Netzwerkbetreiber zu erhalten, der dem eSIM entspricht. Während die vorangegangene Auswahl auf ICCID basiert, wird der Fachmann erkennen, dass andere Typen von Identifizierern verwendet werden können für das eSIM-Management, wobei das ICCID rein veranschaulichend ist.

[0045] Zusätzlich umfasst das sichere Element eine logische Einheit, die beim Verwalten einer Vielzahl von eSIMs nützlich ist, die hiernach als die ”Toolkit”-Anwendung bezeichnet wird. Bei einer beispielhaften Ausführungsform ist die Toolkit-Anwendung eine Advanced Subscriber Identity Toolkit-Softwareanwendung, die intern in dem sicheren Element ausgeführt wird. Jedes eSIM enthält seine eigenen Daten, wie z. B. Telefonbuch-Kontakte, zugeordnete Telefoneinstellungen, Webseiten-Lesezeichen und Dienstprofile für andere Vorrichtungen, mit denen das Gerät kommunizieren kann und/oder die es benutzt. Ein Beispiel von Daten sind z. B. bedingte Umschalt-Präferenzen, die durch den Benutzer (und/oder den Netzwerkbetreiber) definiert sind und die nützlich zum Bestimmen sind, welches eSIM auf der Vorrichtung aktiv sein sollte. Beispielsweise können solche Umschalt-Präferenzen auf der Tageszeit oder dem Wochentag, dem physikalischen Ort der Vorrichtung, einem benutzten Telefonbuch-Kontakt, einem verfügbaren Netzwerkdienst (z. B. ein zellularer Sprach- oder Datennetzwerkdienste), dem Benutzungskontext (z. B. Beruf, persönlich), dem Typ der Kommunikation (z. B. Sprache gegenüber Daten), usw. beruhen.

[0046] Zur Klarstellung, wie hierin verwendet, beziehen sich die Begriffe ”aktiv” und ”inaktiv” auf den Ausführungsstatus des Zugriffssteuerungsclienten und nicht den derzeitigen Verbindungsstatus (d. h. ein aktiver Zugriffssteuerungsclient kann einen Verbindungskontext mit dem Netzwerk haben oder nicht). Daher kann es von den Fachleuten in dem relevanten Fachgebiet begrüßt werden, dass ein Zugriffssteuerungsclient, der durch das sichere Element ausgeführt wird, ”aktiv” ist, wohingegen ein Zugriffssteuerungsclient, der nicht ausgeführt wird, ”inaktiv” ist.

[0047] In einem Ausführungsbeispiel stellt die logische Advanced Subscriber Identity Toolkit-Einheit eine zweite Schnittstelle zwischen den eUICC- und den eSIM-Daten bereit, was dem Gerät erlaubt, auf irgendwelche der eSIM-Daten zuzugreifen, unabhängig davon, welches eSIM aktiv verwendet wird. Als ein kurzer Seitenaspekt erfordern existierende SIM-Karten typischerweise, dass der Benutzer eine Zugriffsbedingung erfüllt (z. B. ein PIN-Code, Passwort, administrativen Code usw.). Außerdem ist bestehenden Vorrichtungen untersagt, mehr als ein aktives SIM zu einem Zeitpunkt zu unterhalten. Demzufolge sind Daten, die in der SIM-Karte gespeichert sind, effektiv nur verfügbar, wenn die SIM-Karte aktiv in Benutzung ist. Im Gegensatz dazu stellt das beispielhafte Advanced Subscriber Identity Toolkit eine zweite Schnittstelle bereit, die unterschiedliche Privilegien und/oder Erlaubnisse von den primären eSIM-Zugriffen hat. Beispielsweise kann das Gerät das Advanced Subscriber Identity Toolkit benutzen, um Telefonbuchkontakte über mehrere eSIMs mit dem Gerät zu suchen und zu teilen. Bei einem anderen Beispiel kann das Advanced Subscriber Identity Toolkit verwendet werden, um automatisches und im Wesentlichen nahtloses Umschalten zwischen unterschiedlichen eSIMs durch Überwachen einer oder mehrerer Bedingungen und Vergleichen der überwachten Bedingungen gegenüber benutzerdefinierten Präferenzen zu erleichtern.

[0048] Bei einer beispielhaften Ausführungsform kann auf das sichere Element **204** nur durch den (die) Baseband-Prozessor(en) **206** direkt zugegriffen werden. Bei solchen Ausführungsbeispielen hat nur der Anwendungsprozessor **202** indirekten Zugriff auf das sichere Element (einschließlich der Toolkit-Anwendung und der Zugriffssteuerungsclienten) über den Baseband-Prozessor. Bei einem alternativen Ausführungsbeispiel sind jedoch sowohl der Anwendungsprozessor **202** als auch der/die Baseband-Prozessor(en) **206** in direkter Kommunikation mit dem sicheren Element **204**. Ein Vorteil, wenn dem Anwendungsprozessor **202** erlaubt wird, direkt mit dem sicheren Element **204** zu kommunizieren, ist eine verbesserte Flexibilität dabei, wie der Anwendungsprozessor **202** Daten speichern und wieder holen kann. Es sollte jedoch vom Fachmann in der relevanten Technik begrüßt werden, dass verschiedene Aspekte der vorliegenden Erfindung darauf gerichtet sind, (i) vielfache Schichten der Zugriffssteuerung und (ii) gleichzeitigen Zugriff bereitzustellen. Daher kann bei einigen Ausführungsbeispielen der Anwendungsprozessor direkt auf die Toolkit-Anwendung zugreifen ohne die Schnittstelle des primären Zugriffssteuerungsclienten zu beeinflussen. Beispielsweise kann ein Benutzer in der Lage sein, nach Kontaktinformation in irgendeinem eSIM zu suchen, ohne notwendigerweise (operationell) zu einem unterschiedlichen eSIM umzuschalten.

[0049] Bei einer beispielhaften Implementierung der vorliegenden Erfindung umfasst die Vorrichtung meh-

rere drahtlose Schnittstellen und Baseband-Prozessoren **206**, die dazu geeignet sind, mit mehreren drahtlosen Netzwerken zu verbinden. Die mehreren drahtlosen Schnittstellen können unterschiedliche Funktechnologien wie z. B. GSM, CDMA, UMTS, LTE/LTE-A, WiMAX, WLAN, Bluetooth usw. durch Implementieren der geeigneten Antennen- und Modemuntersysteme unterstützen. Es wird jedoch begrüßt werden, dass die mehreren Schnittstellen homogen oder heterogen sein können; z. B. kann die Vorrichtung zwei CDMA-Schnittstellen, eine CDMA-Schnittstelle und eine LTE-Schnittstelle, eine WiMAX-Schnittstelle und eine CDMA-Schnittstelle usw. haben.

[0050] Zusätzlich kann bei verschiedenen Ausführungsbeispielen das Gerät **200** ein Benutzerschnittstellen-Untersystem aufweisen, das jede Anzahl von wohl bekannten I/O umfasst, einschließlich, ohne Beschränkung: einer Tastatur, einem Berührungsbildschirm (z. B. einer Vielfachberührungsschnittstelle), eine LCD-Anzeige, Hintergrundbeleuchtung, Lautsprecher und/oder Mikrofon. Es wird jedoch erkannt werden, dass bei bestimmten Anwendungen eine oder mehrere dieser Komponenten weggelassen werden kann. Beispielsweise können Client-Ausführungsbeispiele vom PCMCIA-Kartentyp keine Benutzerschnittstelle haben (da sie auf der Benutzerschnittstelle der Hostvorrichtung huckepack sitzen können, mit der sie physikalisch und/oder elektrisch gekoppelt sind).

[0051] Nun zurück auf **Fig.** 2 Bezug nehmend umfasst in einer beispielhaften Ausführungsform das sichere Element **204** ein nicht-transitorisches computerlesbares Medium, das ein oder mehrere Computerprogramme speichert. Das eine oder die mehreren Computerprogramme sind konfiguriert, um ein erstes Niveau von Vertrauen (oder Privilegien) und/oder ein Zugriffsprotokoll zu implementieren, das unterschiedlich zu dem Vertrauensniveau und dem Zugriffsprotokoll ist, das erforderlich ist, um auf die Zugriffssteuerungsclienten zuzugreifen (z. B. eSIM(s)). Bei einer Variante erlaubt das erste Vertrauensniveau (und/oder Privilegienniveau) einen Softwarezugriff auf die Software des Advanced Subscriber Identity Toolkit und basiert z. B. auf asymmetrischen oder symmetrischen Schlüssel-/Herausforderungsschemata. Beispielsweise kann der Anwendungsprozessor **202** ordnungsgemäß auf eine Herausforderung und ein Antwortschema antworten müssen, um sich selbst als eine gültige Softwareeinheit zu verifizieren. Bei anderen Varianten kann das Zugriffsprotokoll auf einem ordentlich signierten digitalen Zertifikat basieren oder einer anderen Form einer Drittpartei-Verifizierung (z. B. präsentiert der Prozessor ein gültiges Zertifikat und kann danach auf die Software des Advanced Subscriber Identity Toolkit zugreifen). Bei noch anderen Varianten kann die eUICC konfiguriert sein, um eine hardwarespezifische Signatur zu überprüfen, eine hart codierte Vorrichtung oder einen Komponentenidentifizierer (z. B. eine Prozessor-ID usw.). Bei noch anderen Varianten kann das Advanced Subscriber Identity Toolkit in seinen Fähigkeiten beschränkt sein, so dass ein niedrigeres Niveau von Privilegien (oder generische Privilegien) während des Zugriffs verwendet werden kann.

[0052] Bei einer solchen beispielhaften Variante ist das Advanced Subscriber Identity Toolkit mit weniger Restriktionen und schnelleren Fähigkeiten für bestimmte Zugriffstypen konfiguriert (als existierende eSIM-Zugriffe). In einigen Fällen erfordern die reduzierten Restriktionen noch höhere Niveaus von administrativen Privilegien über generische Benutzerprivilegien. Der Fachmann in der relevanten Technik wird leicht erkennen, dass verschiedene Typen von gespeicherter Information, die mit einem eSIM assoziiert sind, mit unterschiedlichen Sicherheitsgraden gehandhabt werden können; beispielsweise kann netzwerkspezifische Kryptografie sehr eng geschützt und kontrolliert werden, wohingegen individuelle Benutzerdaten mit einem niedrigeren Grad an Schutz geschützt werden kann, während generischen oder universellen Daten überhaupt kein Schutz gegeben wird. Während existierende SIM-Karten nur ein einzelnes Zugriffsprotokoll bereitstellen (und daher immer das höchste Sicherheitsniveau erfordern, auch für triviale Transaktionen), kann ein zweites (oder sogar ein drittes) Zugriffsprotokoll für das Advanced Subscriber Identity Toolkit angemessen an die Privilegniveaus der zugeordneten Transaktion angepasst sein (d. h. triviale Transkationen können mit generischen Privilegien durchgeführt werden).

[0053] Beispielsweise betrachte man ein Advanced Subscriber Identity Toolkit, das auf das Hinzufügen, Löschen und/oder Wiederfinden von Kontaktinformation und/oder Manipulieren eines Anrufs und/oder eine Nachrichtenhistorie beschränkt ist. Während die Benutzerinformation vertraulich ist und geschützt sein sollte, wird begrüßt, dass existierende Sicherheits- und administrative Privilegien, die durch den Benutzer verwaltet werden, im Allgemeinen ausreichend zum Schützen der Benutzerinformation sind. Demgemäß kann der Zugriff auf das vorangehende Advanced Subscriber Identity Toolkit auf die gleiche Weise geschützt werden (z. B. über ein vom Benutzer bestimmtes Passwort usw.). Bei einigen Varianten kann das Advanced Subscriber Identity Toolkit weiter mehr stringente Sicherheitsniveaus umfassen, z. B. Buchhaltung und/oder Abrechnungsinformation. Beispielsweise kann ein administratives Privileg erforderlich sein, um sich Abrechnungsinformation anzuschauen. Außerdem kann bei einigen Varianten ein administratives Masterprivileg bereitgestellt werden, z. B. für Servicetechniker und/oder anderes speziell ausgebildetes Personal.

[0054] Bei einem noch anderen Ausführungsbeispiel ist das Advanced Subscriber Identity Toolkit konfiguriert, um Zugriff auf einen gemeinsamen Satz von Daten durch beide eSIMs bereitzustellen und/oder freien Zugriff auf den eSIM-Datensatz für jedes eSIM bereitzustellen. Bei einer Implementierung ist die eUICC mit einem ersten Speicherabschnitt für Netzwerkdaten und eSIM-Daten konfiguriert und einem zweiten Speicherabschnitt für Benutzerdaten. Auf diese Weise hat jedes eSIM Zugriff auf den gemeinsamen Speicherabschnitt während es noch seinen eigenen individuellen Speicher bewahrt. Bei anderen Implementierungen ist die eUICC so konfiguriert, dass jedes eSIM einen unterschiedlichen Speicherraum hat. Bei jeder Implementierung kann das Advanced Subscriber Identity Toolkit verwendet werden, um Zugriff auf Benutzerdaten zu verwalten.

[0055] Die **Fig.** 3 veranschaulicht ein logisches Blockdiagramm einer beispielhaften Ausführungsform einer eingebetteten Universal Integrated Circuit Card (UICC). Wie gezeigt umfasst die eUICC **300** eine erste Schnittstelle für einen eSIM-Zugriff über ein existierendes gemeinsames Betriebssystem **302** (das SIM-Verfahren für sowohl Benutzerdatenzugriff als auch Nicht-Benutzerdatenzugriff erlaubt), und eine zweite Schnittstelle, die in Kommunikation mit dem Advanced Subscriber Identity Toolkit **304** ist. Jedes eSIM **308** hat sowohl für das Toolkit zugreifbare Daten **310** (z. B. benutzerdefinierte Daten, Anwendungen usw.) und nicht für das Toolkit zugreifbare Daten **312** (z. B. kryptografische Information, geschützte Software usw.). Das Advanced Subscriber Identity Toolkit ist konfiguriert, um frei auf den von dem Toolkit zugreifbaren Abschnitt jedes eSIM zuzugreifen. Zusätzlich kann das Advanced Subscriber Identity Toolkit Zugriff auf einen internen (oder externen) gemeinsamen Cachespeicher **306** zum Cachespeichern von Daten usw. haben.

[0056] Bei einigen Ausführungsbeispielen kann das Advanced Subscriber Identity Toolkit **304** zusätzlich einem ersten eSIM erlauben, mit einem zweiten eSIM zu kommunizieren und/oder Daten zu übertragen. Beispielsweise kann ein erstes eSIM **308** eine Anforderung für die Benutzerdaten **310** eines zweiten eSIM ausgeben. Im Allgemeinen wird angenommen, dass der Benutzer der Vorrichtung die ersten und zweiten eSIMs besitzt, daher kann das Advanced Subscriber Identity Toolkit die Anforderung ohne Verifizierung gewähren. Bei einigen Varianten kann das Advanced Subscriber Identity Toolkit jedoch zusätzlich verifizieren, dass das erste eSIM geeignete Privilegien zum Zugreifen auf das zweite eSIM hat. Solche Varianten können nützlich sein, wenn eine Vorrichtung zwischen mehreren Besitzern geteilt wird usw.

[0057] Wie gezeigt sind die erste Schnittstelle für das gemeinsame Betriebssystem **302** und die zweite Schnittstelle für das Advanced Subscriber Identity Toolkit **304** logisch unterschiedlich, es wird jedoch begrüßt, dass die ersten und zweiten Schnittstellen über entweder eine einzelne physikalische Schnittstelle oder unterschiedliche physikalische Schnittstellen implementiert werden können. Bei einigen Ausführungsbeispielen können die ersten und zweiten Schnittstellen an den Baseband-Prozessor **206** gekoppelt sein. Bei anderen Ausführungsbeispielen ist die erste Schnittstelle an den Baseband-Prozessor **206** gekoppelt und die zweite Schnittstelle ist an den Anwendungsprozessor **202** gekoppelt.

Verfahren

[0058] Bezug nehmend nun auf **Fig.** 4 wird ein Ausführungsbeispiel eines verallgemeinerten Verfahrens für die Verwaltung von Daten in einem sicheren Element beschrieben. Bei einer Implementierung der vorliegenden Erfindung sind ein oder mehrere Zugriffssteuerungsclienten in der Lage, Daten zu speichern und wiederzuholen, die nur diesem Zugriffssteuerungsclienten zugeordnet sind. Die Toolkit-Anwendung, die in dem sicheren Element residiert, stellt eine zusätzliche Softwareverwaltungsschicht über die mehreren Zugriffssteuerungsclienten bereit. Die Toolkit-Anwendung hat z. B. ein erstes Privilegniveau und der eine oder die mehreren Zugriffssteuerungsclienten haben ein zweites Privilegniveau. Bei einer Variante kann auf Daten mit entweder dem ersten oder dem zweiten Privilegniveau zugegriffen werden.

[0059] Bei Schritt **402** des Verfahrens **400** bestimmt das sichere Element, ob ein Zugriff auf eine Toolkit-Anwendung gerichtet ist oder auf einen oder mehrere Zugriffssteuerungsclienten. Wenn der Zugriff auf einen Zugriffssteuerungsclienten gerichtet ist (z. B. ein eSIM), dann stellt das sichere Element Zugriff auf den Zugriffssteuerungsclienten über z. B. ISO 7816, ISO 14443, USB usw. bereit. Andererseits, wenn der Zugriff auf die Toolkit-Anwendung gerichtet ist, dann geht das Verfahren zu Schritt **404** weiter.

[0060] Bei einem Ausführungsbeispiel hat das sichere Element eine einzelne Schnittstelle, die logisch in (i) die Toolkit-Anwendung und (ii) die Zugriffssteuerungsclienten-Anwendungen aufgeteilt ist. Beispielsweise umfassen SIM-Kartenschnittstellen typischerweise einen Takt, ein Rücksetzen und eine einzelne Eingabe/Ausgabe (IO). Die IO-Leitung ist getaktet, um zu lesen und zu schreiben (und kann interpretiert werden als Daten, Adressen und/oder Befehle). Die Toolkit-Anwendung kann mit einer Serie von spezialisierten Befehlen versehen sein, einem unterschiedlichen Speicheradressraum, einem Betriebsmodusschalter usw. Beispielsweise kann ein sicheres Element eine einzelne gemeinsame Schnittstelle haben, die sowohl SIM-Kartenzugriffe als auch Toolkit-Anwendungszugriffe akzeptiert. Bei anderen beispielhaften Konfigurationen wird das sichere Element

physikalisch oder logisch zwischen SIM-Kartenzugriffen und Toolkit-Anwendungszugriffen umgeschaltet (z. B. durch Schreiben zu einem Auswahlregister, Setzen eines Modusschalters usw.).

[0061] Bei anderen Ausführungsbeispielen ist das sichere Element mit einer unterschiedlichen physikalischen Schnittstelle für jede der Toolkit-Anwendungen und der Zugriffssteuerungsclienten-Anwendungen versehen (d. h. zwei Schnittstellen). Beispielsweise, wie zuvor angegeben, kann eine SIM-Kartenschnittstelle einen Takt, ein Rücksetzen und eine einzelne Eingabe/Ausgabe (IO) umfassen, wohingegen ein getrennter Adress- und Datenbus für den Toolkit-Zugriff verwendet wird. Es wird auch begrüßt werden, dass die zwei oder mehreren Schnittstellen ein oder mehrere gemeinsame Merkmale teilen können (z. B. Teilen eines Taktes und Rücksetzen, aber Verwenden von getrennten Daten/Adressbussen).

[0062] Bei einer Variante ist der Anforderer ein Benutzer. Beispielsweise kann ein Benutzer Zugriff auf Telefonbuch-Kontakte anfordern, die einem (oder einer Untermenge) des einen oder der mehreren Zugriffssteuerungsclienten zugeordnet sind. Im Allgemeinen wird begrüßt, dass ein Benutzer solche Anforderungen über eine grafische Benutzerschnittstelle (GUI) durchführen wird, die von dem Anwendungsprozessor ausgeführt wird; andere Formen von Schnittstellen sind jedoch in Übereinstimmung mit der Erfindung möglich. Beispielsweise kann die Vorrichtung einen exponierten Knopf oder eine andere physikalische Einrichtung zum Auslösen bestimmter Operationen haben (z. B. SIM-Sperre, SIM-Austausch usw.).

[0063] Bei einer anderen Variante kann der Anforderer eine Softwareanwendung sein, die auf einem Prozessor der Vorrichtung ausgeführt wird. Beispielsweise, wenn eSIM-Daten verwendet werden, um eine automatische Umschaltung zwischen mehreren eSIMs zu erleichtern, kann ein Baseband-Prozessor und/oder Modem der Host-Funkvorrichtung (z. B. Smartphone) gespeicherte Datenumschaltkriterien für jedes eSIM anfordern, um beim automatischen Bestimmen zu assistieren, welches bestimmte eSIM aktiv auf der Vorrichtung sein sollte. Bei anderen Beispielen können eSIM-Daten durch einen Anwendungsprozessor angefordert werden, um beim persönlichen Kontaktinformationsmanagement zu assistieren usw.

[0064] Bei noch einer anderen Variante kann der Anforderer Software sein, die intern durch das eSIM selbst ausgeführt wird, oder ein anderes eSIM. Beispielsweise kann ein erstes eSIM eine Synchronisierung von persönlichen Kontaktinformationen mit einem zweiten eSIM anfordern. Bei noch anderen Beispielen kann ein erstes eSIM automatisch sich selbst in Übereinstimmung mit Vorrichtungseinstellungen konfigurieren, die mit einem zweiten eSIM assoziiert sind, wie z. B. eine anfängliche Hinzufügung des ersten eSIM zu einer UICC.

[0065] Der Fachmann in der relevanten Technik wird erkennen, dass Software einen breiten Bereich von Funktionalitäten, Fähigkeiten und/oder Privilegien überspannt. Bekannte Beispiele von Software umfassen, ohne Einschränkung: Firmware, Vorrichtungstreiber auf niedrigem Niveau, Betriebssystemtreiber (OS), native Vorrichtungsanwendungen, Drittpartei-Softwareanwendungen, vernetzte Anwendungen und virtuelle Maschinen. Demgemäß kann bei einigen Ausführungsbeispielen der vorliegenden Erfindung die Toolkit-Anwendung weiter unterschiedliche Softwarefähigkeiten basierend auf dem Typ der Software des Anforderers herausstellen. Beispielsweise können einem Vorrichtungstreiber auf niedrigem Niveau unterschiedliche Fähigkeiten und Funktionen gegeben werden als, z. B. einer vernetzten Anwendung.

[0066] Als eine kurze Randbemerkung umfassen bekannte Bespiele von Daten ohne Beschränkung: bedingte Betriebskriterien für Zugriffssteuerungsclienten (z. B. Einstellungen für automatisches SIM-Umschalten usw.), Webseitenlesezeichen, Account-Passwortlisten, Anruf und/oder Nachrichtenhistorie, Benutzer- oder finanzielle Account-Information, Vorrichtungsprofileinstellungen, Softwareanwendungen usw.

[0067] Bekannte Beispiele von unterstützten Datenzugriffen umfassen, aber sind nicht darauf beschränkt: Wiedergewinnen von Daten, Speichern von Daten, Modifizieren von Daten (z. B. Überschreiben oder Ersetzen), Ausführen von Befehlen, Bestimmen der Datenvalidität (z. B. Durchführen einer zyklischen Redundanzüberprüfung (CRC), kryptografischer Einweg-Hash, oder eine andere Integritätsüberprüfung), Erlauben/Sperren von Merkmalen usw. Außerdem wird begrüßt, dass bestimmte Typen von Zugriffen komplex sein können und/oder erfordern, dass die Toolkit-Anwendung vielfache interne Transaktionen durchführt. Tatsächlich ist ein herausragender Vorteil der hier offenbarten beispielhaften Toolkit-Anwendung, dass komplexe Transaktionen intern an dem sicheren Element durchgeführt werden können. Existierender SIM-Kartenzugriff wird über ISO 7816 Signalisieren durchgeführt, das sehr viel langsamer ist als der eigene interne Zugriff des sicheren Elements. Beispielsweise basiert eine einfache Leseanforderung über das ICC ISO 7816 Protokoll auf einer verhandelten Geschwindigkeit und kann maximal mehrere hundert kbps (Kilobits pro Sekunde) erreichen.

[0068] Bei Schritt **404** wird die Anforderung, auf Daten zuzugreifen, optional für geeignete Erlaubnisse, Privilegien und/oder Verhalten durch die Toolkit-An-

wendung verifiziert. Allgemeiner führt die Toolkit-Anwendung nur Zugriffe entsprechend dem Niveau des Privilegs durch, das durch den Anforderer gewährt ist; diese Einschränkung stellt sicher, dass die Vertrauensgrenze des sicheren Elements und der Zugriffssteuerungsclienten nicht durch eine ungeschickte oder böswillige Benutzung der Toolkit-Anwendung umgangen werden kann. Bei einem Ausführungsbeispiel greift die Toolkit-Anwendung nur auf eine Untermenge des gesamten Bestandes des sicheren Elements zu. Bei einer Variante ist die Untermenge auf die Daten beschränkt, die dem Privileg des Anforderers entsprechen. Bei anderen Varianten hat die Toolkit-Anwendung selbst ein maximales Privilegniveau. Beispielsweise kann die Toolkit-Anwendung nur dazu in der Lage sein, benutzerdefinierte Daten zu modifizieren und auf sie zuzugreifen.

[0069] Beispielsweise kann ein Benutzer eine Vereinigung eines ersten Telefonbuchs, dass einem ersten eSIM zugeordnet ist, und eines zweiten Telefonbuchs, das einem zweiten eSIM zugeordnet ist, anfordern. Die Toolkit-Anwendung kann zusätzlich eine geeignete Zugriffs-PIN für eine oder beide der eSIMs anfordern (oder den Benutzer dazu anregen). Bei anderen Beispielen kann der Benutzer Zugriff auf Abrechnungsinformation anfordern, die einem eSIM zugeordnet ist. Reagierend kann die Toolkit-Anwendung bei dem Benutzer nach einem Passwort (oder PIN) nachfragen, bevor Kreditkarteninformation bereitgestellt wird. Bei noch einem anderen Beispiel kann eine Drittpartei-Anwendung Benutzerdaten des eSIM anfordern, um bestimmte Funktionalitäten zu erlauben (z. B. In-App-Zahlungen, Benutzerhistorie-Statistiken usw.), die Toolkit-Anwendung kann verifizieren, dass die Drittpartei-Anwendung eine Erlaubnis bekommen hat, auf die persönliche Information des Benutzers zuzugreifen, bevor die angeforderten Daten bereitgestellt werden.

[0070] Wenn die Toolkit-Anwendung bestimmt, dass eine unzureichende Erlaubnis vorliegt, um auf Daten zuzugreifen, dann wird die Anforderung nach Zugriff abgelehnt (Schritt **406**). Bei einigen Varianten kann eine Fehlernachricht an die anfordernde Einheit (z. B. Benutzer, Software, Netzwerkeinheit usw.) bereitgestellt werden. Ansonsten, wenn die Toolkit-Anwendung bestimmt, dass eine ausreichende Erlaubnis vorliegt, wird die Anforderung nach Zugriff gewährt (Schritt **408**).

[0071] Außerdem wird der Fachmann in der relevanten Technik erkennen, dass die sensitive Natur von Inhalten des Zugriffssteuerungsclienten zusätzliche Schichten von Sicherheit erfordern kann, um böswillige Angriffe zu verhindern. Beispielsweise können verschiedene Ausführungsbeispiele der vorliegenden Erfindung konfiguriert sein, um zusätzlich unter anderem Eingabevalidierungen (d. h. Anforderungen sind gut formiert und erfüllen erwartete Eingaben), Authentifizierung/Autorisierung, Integritätsüberprüfung, Sitzungsmanagement (z. B. eine Sitzung bleibt nicht offen oder greift auf Inhalten falsch zu, usw.), Ausnahmeverwaltung (d. h. Fehlerbedingungen werden geeignet gehandhabt), und/oder Auditing/Logging durchzuführen.

[0072] Bei einem anderen Beispiel kann eine Anforderung autorisiert werden gemäß einem Zertifikat. Beispielsweise kann die Anforderer-Software ein Zertifikat präsentieren müssen, das von einer vertrauenswürdigen dritten Partei unterzeichnet ist, was anzeigt, dass die Anforderer-Software für den angeforderten Zugriff autorisiert ist. Ein Beispiel solch eines Zertifikats umfasst eine Unterschrift (einer vertrauenswürdigen dritten Partei), die mit einer Software-Identifizierung und/oder Vorrichtungsidentifizierung gehasht worden ist. Bei einem anderen solchen Beispiel wird die Anforderung gemäß dem Privilegniveau der Anforderer-Software verifiziert. Beispielsweise kann man ein System betrachten, bei dem das Betriebssystem ein erstes Privilegniveau, Drittpartei-Software ein zweites Privilegniveau und der Kommunikationssoftwarestapel noch ein anderes Privilegniveau hat. Bei einigen Varianten kann der Benutzer zusätzlich dazu in der Lage sein, eines oder mehrere Privilegniveaus zu konfigurieren (z. B. bestimmten Drittpartei-Anwendungen mehr Zugriff zu gewähren oder Privilegien davon zurückzuziehen).

[0073] In noch anderen Fällen kann das Anwendungs-Toolkit verifizieren, dass die Anforderer-Software in Übereinstimmung mit akzeptierbarem Benehmen operiert. Gemeinsame Überprüfungen umfassen ohne Beschränkung: Verifizieren einer Eingabe für Übereinstimmung nach Format und Länge, Sitzungs-Timeout-Funktionen, geeignete Speicheroperation (z. B. Verhindern von weglaufenden Zeigern usw.), usw.

[0074] Bei Schritt **408** des Verfahrens **400** greift die Toolkit-Anwendung auf die angeforderten Daten des Zugriffssteuerungsclienten zu. Bei einem Ausführungsbeispiel greift die Toolkit-Anwendung auf den Speicherraum des geeigneten Zugriffssteuerungsclienten direkt zu. Beispielsweise ist eine speicherabgebildete Dateistruktur typisch gemäß vordefinierten Aufteilungen angeordnet. Bei einer solchen Variante sind die Aufteilungen aufgeteilt in: (i) benutzerdefinierte Daten (UDD), und (ii) Nicht-Benutzerdaten (z. B. kryptografische Daten, Software, Firmware, usw.). Um einen Zugriff durchzuführen bestimmt das Toolkit die geeignete Speicheradresse von einer zuvor gecachten Inhaltsverzeichnisstruktur oder durch schrittweises Durchgehen der Inhaltsverzeichnisstruktur bis der Speicherort gefunden ist. Bei alternativen Ausführungsbeispielen greift die Toolkit-Anwendung auf den Zugriffssteuerungsclienten über einen Satz von Zugriffssteuerungsclienten-spezifischen Anweisungen zu. Dateistrukturen vom SIM-

Typ werden gewöhnlicherweise verschleiert, um einen direkten Zugriff auf gespeicherte Daten zu verhindern. Daher muss in einigen Ausführungsbeispielen die Toolkit-Anwendung auf die Dateistruktur unter Verwendung des nativen Befehlssatzes der SIM-Vorrichtung zugreifen. Während solch ein indirekter Zugriff mehr Zeit als direkte Zugriffsverfahren erfordern kann, erfordert die Toolkit-Schnittstelle vorteilhafterweise nicht viele der Protokollsicherungen, die andererseits bei Verwendung von Techniken des Standes der Technik durchgeführt werden müssten.

[0075] Bei einigen Ausführungsbeispielen greift die Toolkit-Anwendung auf einen gemeinsamen Speicherraum zu. Gemeinsame Speicherräume können zeitlich voraus mit Daten vorgecacht werden oder können auf einer wie benötigt oder wie benutzt Basis belegt werden. Im Allgemeinen ist Cache-Speicher kleiner und auf ihn kann schneller zugegriffen werden als auf traditionelle Speicherstrukturen, aber er muss optimiert werden, um Cache-"Versäumnisse" zu reduzieren (wenn der Cache nützliche Daten hat) und Cache-"Treffer" zu maximieren (wenn der Cache keine nützlichen Daten hat). Zu diesen Zwecken implementieren Cache-Speicher unterschiedliche Ersetzungspolitiken; spezifisch bei einem Cache-Versäumnis kann der Cache einen seiner existierenden Einträge mit den wiedergeholten validen Daten ersetzen. Austauschstrategien bestimmen, welcher existierende Cache-Eintrag mit der geringsten Wahrscheinlichkeit in der Zukunft benutzt werden wird. Bei einer Variante tauscht der Cache Einträge gemäß einem am wenigsten kürzlich-benutzt (LRU) Paradigma aus, d. h. bei einem Cache-Versäumnis tauscht der Cache den am wenigsten kürzlich zugegriffenen Eintrag mit den Daten aus, die, z. B. von dem Zugriffssteuerungsclienten wiedergeholt worden sind.

[0076] Bei Schritt **410** wird das Ergebnis des Zugriffs dem Anforderer zurückgegeben. Bei einigen Varianten kann die Toolkit-Anwendung zusätzlich Zugriffe anmelden, den Cache aktualisieren und/oder Einlog-Information dem Zugriffssteuerungsclienten bereitstellen.

[0077] Der Fachmann in der relevanten Technik wird im Hinblick auf die vorliegende Offenbarung erkennen, dass verschiedene Aspekte der vorliegenden Erfindung Zugriff auf Daten über eine intern gesteuerte Toolkit-Anwendung bereitstellen, die sicher innerhalb des sicheren Elements ausgeführt wird (und der inhärent vertraut werden kann).

Beispiel Telefonbuchverschmelzung

[0078] **Fig.** 5 veranschaulicht eine bestimmte Implementierung eines Verfahrens **500** zum Verschmelzen von benutzerdefinierten Kontaktinformationen mehrerer elektronischer Subscriber Identity Module (eSIMs). Man betrachte das Szenario, bei dem ein eSIM A ein Telefonbuch mit 200 Einträgen hat und ein eSIM B ein Telefonbuch mit 300 Einträgen hat und das eSIM A und das eSIM B 100 überlappende Einträge haben.

[0079] Bei Schritt **502** identifiziert ein Benutzer eines Smartphones (wie z. B. das beispielhafte iPhone™, das durch den Anmelder hergestellt wird), zwei (2) eSIMs (eSIM A, eSIM B) und gibt eine Anforderung heraus, die Kontaktinformation der beiden eSIMs zu verschmelzen, über eine grafische Benutzerschnittstelle (GUI), die von einem Anwendungsprozessor ausgeführt wird. Bei diesem Beispiel ist die Anforderung auf eine Advanced Subscriber Identity Toolkit-Anwendung gerichtet, die von dem sicheren Element der eingebetteten Universal Integrated Circuit Card (eUICC) ausgeführt wird.

[0080] Bei Schritt **504** verifiziert das Advanced Subscriber Identity Toolkit, dass der anfordernde Benutzer die geeigneten Privilegien hat, um die Kontaktinformation zu verschmelzen. Die Verifizierung des Privilegs kann z. B. auf einer von dem Benutzer gelieferten PIN (oder PINs) basieren, einem Passwort, vertrauenswürdigem Berechtigungsnachweis, der durch einen Drittpartei-Authentifizierer bereitgestellt worden ist usw. Es wird jedoch geschätzt werden, dass eine solche Verifizierung des Privilegs des Benutzers unnötig sein kann und in bestimmten Fällen, wenn erwünscht, übersprungen werden kann.

[0081] Bei Schritt **506** holt das Advanced Subscriber Identity Toolkit die 200 Einträge von dem eSIM A und die 300 Einträge von dem eSIM B und führt eine interne Verschmelzung der Einträge durch. Es ist wert darauf hinzuweisen, dass Dual-SIM-Vorrichtungen des Standes der Technik notwendigerweise sich bei der ersten SIM-Karte authentifizieren müssen, um den ersten Satz von Einträgen auszulesen, und darauffolgend sich bei der zweiten SIM-Karte authentifizieren müssen, um den zweiten Satz von Einträgen auszulesen. Schlimmer noch würden Lösungen des Standes der Technik erfordern, die vorangehenden Operationen vollständig über die ISO 7816-Kartenschnittstelle durchzuführen, die wie zuvor angemerkt, signifikant langsamer als der interne Speicherzugriff ist, der durch die Toolkit-Anwendung ermöglicht wird.

[0082] Bezug nehmend auf **Fig.** 5 gibt bei Schritt **508** das Advanced Subscriber Identity Toolkit die verschmolzene Liste von 400 Einträgen zurück, die in dem Speicher gespeichert ist (z. B. durch den Anwendungsprozessor). Der Benutzer wird informiert, sobald die Verschmelzung vervollständigt ist.

Beispiel Kontaktsuche

[0083] **Fig.** 6 veranschaulicht eine bestimmte Implementierung eines Verfahrens **600** zum Suchen von

Kontaktinformation innerhalb einer oder mehrerer elektronischer Subscriber Identity Module (eSIMs).

[0084] Bei Schritt **602** fordert ein Benutzer eines Smartphones Kontaktinformation für "John Doe" an. Bei diesem Beispiel hat der Benutzer keine Ziel-eSIM bereitgestellt, es wird jedoch begrüßt, dass, wenn der Benutzer eine Ziel-eSIM bereitgestellt hat, die Suche signifikant eingeschränkt werden kann.

[0085] Wenn notwendig verifiziert bei Schritt **604** das Advanced Subscriber Identity Toolkit, dass der anfordernde Benutzer (oder die anfordernde Anwendung) die geeigneten Privilegien hat, um den angegebenen Kontakt zu suchen. Bei einigen Varianten kann das Advanced Subscriber Identity Toolkit die Untermenge von eSIMs identifizieren, die suchbar ist, basierend auf den Erlaubnissen des anfordernden Benutzers (oder der Anwendung).

[0086] Bei Schritt **606** sucht das Advanced Subscriber Identity Toolkit die eSIMs für passende Einträge. Als eine kurze Randbemerkung, während existierende SIM-Karten einzelne Eintragszugriffe erlauben, würde bei diesem bestimmten Szenario Software des Standes der Technik, den gesamten Satz von Kontakten lesen müssen, um eine Suche in dem Anwendungsprozessor durchzuführen. Insbesondere ist ein Index für einen bestimmten Eintrag unbekannt, existierende Software muss den gesamten Satz von Einträgen aus der UICC auslesen und eine Suche unter den Einträgen durchführen, die ausgelesen worden sind.

[0087] Bezug nehmend zurück auf **Fig.** 6 gibt bei Schritt **608** das Advanced Subscriber Identity Toolkit die lokalisierten Kontaktinformationsergebnisse an den anfordernden Benutzer oder die Anwendung zurück.

Beispiel einer Umschaltoperation

[0088] **Fig.** 7 veranschaulicht eine bestimmte Implementierung des Verfahrens von **700** zum Erleichtern eines automatischen Umschaltens zwischen elektronischen Subscriber Identity Modulen (eSIMs) basierend auf einem benutzerdefinierten bedingten Auslöser.

[0089] Bei Schritt **702** des Verfahrens **700** definiert ein Benutzer eines Smartphones einen bedingten Auslöser, um automatisch zwischen eSIMs zu einem bestimmten Zeitpunkt des Tages umzuschalten entsprechend z. B. einer Benutzung oder einem anderen Kontext. Beispielsweise kann ein Benutzer auswählen, ein erstes eSIM A zwischen 7 Uhr morgens und 5 Uhr abends (z. B. einen Arbeits-Account) freizugeben, und ein zweites eSIM B zwischen 5 Uhr abends und 7 Uhr morgens (z. B. einen persönlichen Account). Der bedingte Umschaltauslöser wird als Benutzerpräferenzdaten in jeder jeweiligen eSIM gespeichert.

[0090] Bei Schritt **704** überprüft das Advanced Subscriber Identity Toolkit die Benutzerpräferenzdaten der bedingten Auslöser nach Validität. Beispielsweise kann das Advanced Subscriber Identity Toolkit sicherstellen, dass ein und nur ein eSIM für alle Zeiten definiert ist (d. h. es gibt keine Überlappungen). Wenn die bedingten Auslöser valide sind, dann konfiguriert das Advanced Subscriber Identity Toolkit seine Auslösefähigkeit und konfiguriert jedes der eSIMs in geeigneter Weise (d. h. Gewährleisten, dass die eSIMs bei ihrer geeigneten Benutzungszeit freigegeben sind, oder dass die Umschaltung nicht in der Mitte einer operationellen Transaktion, wie z. B. einem Anruf oder beim Herunterladen, durchgeführt wird).

[0091] Der Fachmann in der relevanten Technik wird erkennen, dass SIM-Karten des Standes der Technik nicht die vorangegangenen Fähigkeiten haben. Außerdem können Dual-SIM-Vorrichtungen des Standes der Technik nicht auf diese Weise zusammenarbeiten, da beide SIM-Karten unterschiedliche logische Einheiten sind, die nicht in der Lage sind, miteinander zu kooperieren oder den Betrieb der anderen zu diktieren oder zu beeinflussen.

[0092] Bei Schritt **706** überwacht das Advanced Subscriber Identity Toolkit die Auslösebedingung (z. B. eine Zeit, ein Ereignis usw.). Beispielweise, wenn die Tageszeit (gemäß einer internen Taktreferenz oder durch eine externe Netzwerksignalisierung) die 5 Uhr abends Bedingung erfüllt, schaltet das Advanced Subscriber Identity Toolkit von dem ersten eSIM A zu dem zweiten eSIM B um, ähnlich, wenn die 7 Uhr abends Bedingung erfüllt ist, schaltet das Advanced Subscriber Identity Toolkit von dem zweiten eSIM B auf das erste eSIM A um.

[0093] Bei einigen Varianten gibt die eUICC (oder das Advanced Subscriber Identity Toolkit) eine "Auffrisch"-Anweisung an den Baseband-Prozessor; in Reaktion darauf frischt der Baseband an die Dateistruktur der neuen eSIM auf und führt AKA-Prozeduren durch. Bei einigen Fällen kann jede solche Aktion, die während einer laufenden operationellen Bedingung aufgerufen wird, wie z. B. einem Anruf, ausgesetzt oder vertagt werden, bis zur Beendigung dieser Bedingung.

[0094] Es wird auch begrüßt werden, dass Zugriffe auf das "Telefonbuch" des eSIM des Beispiels der **Fig.** 5 hierin als eine Auslösebedingung für einen Kontextwechsel (und daher des eSIM) verwendet werden kann. Beispielsweise kann eine Telefonbuchanwendung des Benutzers, die auf dem Anwendungsprozessor läuft, bestimmte Kontakte als "persönlich" markiert oder gekennzeichnet haben und andere als "beruflich". Alle beruflichen Kontakte des Be-

nutzers können auf einem beruflichen eSIM angeordnet sein und alle persönlichen Kontakte auf einem persönlichen eSIM; demgemäß kann eine Auswahl des Benutzers eines Kontakts das Toolkit dazu führen, ein bestimmtes eSIM oder "Identität" auszuwählen, wenn es nicht schon in Benutzung ist.

[0095] Es wird erkannt werden, dass, während bestimmte Aspekte der Erfindung in Begriffen einer spezifischen Folge von Schritten eines Verfahrens beschrieben worden sind, diese Beschreibung nur veranschaulichend für die breiteren Verfahren der Erfindung sind und modifiziert werden können, wenn dies durch die bestimmte Anwendung erforderlich ist. Bestimmte Schritte können unter bestimmten Umständen unnötig werden oder optional. Zusätzlich können bestimmte Schritte oder Funktionalitäten den offenbarten Ausführungsbeispielen hinzugefügt werden oder die Reihenfolge der Durchführung von zwei oder mehreren Schritten kann ausgetauscht werden. Alle solche Varianten werden als von der hierin offenbarten und beanspruchten Erfindung umfasst betrachtet.

[0096] Während die obige detaillierte Beschreibung neue Merkmale der Erfindung, wie sie bei verschiedenen Ausführungsbeispielen angewandt werden, gezeigt, beschrieben und herausgestrichen hat, wird verstanden werden, dass verschiedene Weglassungen, Ersetzungen und Wechsel in der Form und Details der Vorrichtung oder des veranschaulichten Verfahrens durch den Fachmann gemacht werden können, ohne von der Erfindung abzuweichen. Die vorangehende Beschreibung ist die beste Art, die derzeit zum Ausführen der Erfindung in Erwägung gezogen wird. Diese Beschreibung ist in keiner Weise gedacht, beschränkend zu sein, sondern sollte als Veranschaulichung der allgemeinen Prinzipien der Erfindung genommen werden. Der Schutzbereich der Erfindung sollte mit Bezug auf die Ansprüche bestimmt werden.

Patentansprüche

1. Eine mobile Vorrichtung, die aufweist:
drahtlose Schaltung, die angepasst ist, mit zumindest einem drahtlosen Netzwerk zu kommunizieren;
ein sicheres Element, das konfiguriert ist, um eine Mehrzahl von Zugriffssteuerungsclienten zu speichern,
wobei die Mehrzahl von Zugriffssteuerungsclienten zumindest einen aktiven Zugriffssteuerungsclienten und einen inaktiven Zugriffssteuerungsclienten umfasst;
Logik, die konfiguriert ist, um an das sichere Element eine Anforderung auszugeben, um auf eine Datenkomponente zuzugreifen, die in dem inaktiven Zugriffssteuerungsclienten enthalten ist, ohne zu fordern, dass der inaktive Zugriffssteuerungsclienten aktiviert wird; und
Logik, die konfiguriert ist, um von dem sicheren Element die Datenkomponente zu empfangen, wenn das sichere Element verifiziert, dass die Anforderung gültig ist.

2. Mobile Vorrichtung gemäß Anspruch 1, weiter aufweisend:
Logik, die konfiguriert ist, um zumindest einen Teil der Datenkomponenten zu zumindest einem Zugriffssteuerungsclienten der Mehrzahl von Zugriffssteuerungsclienten zu transferieren,
wobei der zumindest eine Zugriffssteuerungsclient nicht den inaktiven Zugriffssteuerungsclienten umfasst.

3. Mobile Vorrichtung gemäß Anspruch 2, wobei der zumindest eine Zugriffssteuerungsclient den aktiven Zugriffssteuerungsclienten umfasst.

4. Mobile Vorrichtung gemäß einem der Ansprüche 1 bis 3, wobei die Anforderung einen Anforderer identifiziert, der die Anforderung generiert.

5. Mobile Vorrichtung gemäß Anspruch 4, wobei der Anforderer einen Benutzer umfasst.

6. Mobile Vorrichtung gemäß Anspruch 4, wobei der Anforderer eine Software-Anwendung umfasst.

7. Mobile Vorrichtung gemäß Anspruch 6, wobei die Software-Anwendung auf dem sicheren Element residiert.

8. Mobile Vorrichtung gemäß Anspruch 4, wobei der Anforderer einen Software-Prozess aufweist, der auf dem aktiven Zugriffssteuerungsclienten resident ist.

9. Verfahren zum Verwalten einer Mehrzahl von Zugriffssteuerungsclienten, die in einem sicheren Element gespeichert sind, wobei das Verfahren aufweist:
Empfangen von einem Anforderer einer Anforderung, auf eine Datenkomponente zuzugreifen, die in einem bestimmten Zugriffssteuerungsclienten der Mehrzahl von Zugriffssteuerungsclienten enthalten ist;
Verifizieren der Anforderung;
Durchsuchen der Mehrzahl von Zugriffssteuerungsclienten für den bestimmten Zugriffssteuerungsclienten;
Erhalten zumindest eines Abschnitts der Datenkomponente von dem bestimmten Zugriffssteuerungsclienten; und
Zurückgeben zumindest eines Abschnitts der Datenkomponente an den Anforderer.

10. Verfahren gemäß Anspruch 9, wobei das Verifizieren der Anforderung Authentifizieren des Anforderers umfasst.

11. Verfahren gemäß Anspruch 10, wobei das Verifizieren der Anforderung weiter Analysieren eines Privilegniveaus umfasst, das dem Anforderer zugeordnet ist.

12. Verfahren gemäß Anspruch 11, wobei das Privilegniveau, das dem Anforderer zugeordnet ist, durch eine administrative Einheit vorbestimmt ist.

13. Verfahren nach einem der Ansprüche 9 bis 12, wobei:
die Datenkomponente Kontaktinformation für eine Mehrzahl von Individuen aufweist;
die Anforderung ein bestimmtes Individuum aus der Mehrzahl von Individuen spezifiziert; und
der zumindest eine Abschnitt der Datenkomponente Kontaktinformation für das bestimmte Individuum aufweist.

14. Verfahren gemäß einem der Ansprüche 9 bis 12, wobei der zumindest eine Abschnitt der Datenkomponente Vorrichtungskonfigurationsinformation für eine mobile Vorrichtung aufweist, in der das sichere Element umfasst ist, und wobei das Verfahren weiter aufweist:
Konfigurieren eines Betriebszustands der mobilen Vorrichtung basierend auf der Vorrichtungskonfigurationsinformation.

15. Ein sicheres Element, das konfiguriert ist, um eine Mehrzahl von Zugriffssteuerungsclienten zu verwalten, aufweisend:
Mittel zum Empfangen, von einem Anforderer, einer Anforderung, auf eine Datenkomponente zuzugreifen, die in einem bestimmten Zugriffssteuerungsclienten der Mehrzahl von Zugriffssteuerungsclienten enthalten ist;
Mittel zum Verifizieren der Anforderung;
Mittel zum Durchsuchen des bestimmten Zugriffssteuerungsclienten nach der darin gespeicherten Datenkomponente; und
Mittel zum Zurückgeben der Datenkomponente zu dem Anforderer.

16. Sicheres Element gemäß Anspruch 15, wobei der Anforderer ein Benutzer ist und das Verifizieren der Anforderung das Verifizieren einer persönlichen Identifizierungsnummer (PIN) oder ein Passwort, das von dem Benutzer geliefert wird, umfasst.

17. Sicheres Element gemäß Anspruch 15, wobei der Anforderer eine Software-Anwendung ist und Verifizieren der Anforderung Analysieren eines Privilegniveaus umfasst, das Eigenschaft der Software-Anwendung ist.

18. Sicheres Element gemäß Anspruch 15, das weiter Mittel zum Authentifizieren gegenüber einem Netzwerk aufweist, das zumindest einen Zugriffssteuerungsclienten der Mehrzahl von Zugriffssteuerungsclienten benutzt.

19. Eine mobile Vorrichtung, die aufweist:
drahtlose Schaltung, die angepasst ist, um mit einem drahtlosen Netzwerk zu kommunizieren;
einen Prozessor;
eine Speichervorrichtung in Datenkommunikation mit dem Prozessor, wobei die Speichervorrichtung computerausführbare Anweisungen speichert, die konfiguriert sind, um, wenn sie durch den Prozessor ausgeführt werden, den Prozessor dazu zu veranlassen:
an ein sicheres Element, das in der mobilen Vorrichtung umfasst ist und konfiguriert ist, um eine Mehrzahl von Zugriffssteuerungsclienten zu speichern, eine Anforderung zu übertragen, auf eine Datenkomponente zuzugreifen, die in einem bestimmten Zugriffssteuerungsclienten der Mehrzahl von Zugriffssteuerungsclienten enthalten ist, wobei die Anforderung ein bestimmtes Privilegniveau spezifiziert, das Zugriff auf die Datenkomponente erlaubt; und
das sichere Element, wobei das sichere Element konfiguriert ist, um:
die Anforderung zu verifizieren;
auf die Datenkomponente des bestimmten Zugriffssteuerungsclienten zuzugreifen; und
die Datenkomponente zu dem Prozessor zurückzugeben.

20. Verfahren zum Zugreifen auf eine Datenkomponente, die in einem Zugriffssteuerungsclienten enthalten ist, der in einem sicheren Element einer Benutzervorrichtung gespeichert ist, aufweisend:
an einem Prozessor, der in der Benutzervorrichtung umfasst ist, Übertragen einer Anforderung zu dem sicheren Element, um auf die Datenkomponente zuzugreifen, wobei das sichere Element eine Mehrzahl von Zugriffssteuerungsclienten speichert, die den Zugriffssteuerungsclienten umfasst, und wobei das Zugriffssteuerungsclient inaktiv ist;
bei dem sicheren Element, Verifizieren der Anforderung und, wenn die Anforderung gültig ist, Zugreifen auf die Datenkomponenten und Bereitstellen der Datenkomponente zu dem Prozessor;
an dem Prozessor, Empfangen der Datenkomponente von dem sicheren Element; und
an dem Prozessor, Modifizieren des Betriebszustands der Benutzervorrichtung basierend auf der empfangenen Datenkomponente.

21. Ein sicheres Element, das konfiguriert ist, um eine Mehrzahl von Zugriffssteuerungsclienten zu speichern, wobei jeder Zugriffssteuerungsclient der Mehrzahl von Zugriffssteuerungsclienten eine Datenkomponente enthält, wobei das sichere Element aufweist:
einen sicheren Prozessor; und
eine sichere Speichervorrichtung in Datenkommunikation mit dem sicheren Prozessor, wobei die sichere Speichervorrichtung computerausführbare Anwei-

sungen speichert, die konfiguriert sind, um, wenn sie durch den sicheren Prozessor ausgeführt werden, den sicheren Prozessor dazu zu veranlassen:
von einem Anforderer eine Anforderung zu empfangen, auf die Datenkomponente eines Zugriffssteuerungsclienten der Mehrzahl von Zugriffssteuerungsclienten zuzugreifen, wobei der Zugriffssteuerungsclient inaktiv ist und die Anforderung Privilegniveau-Information umfasst, die dem Anforderer zugeordnet ist;
die Anforderung basierend auf der Privilegniveau-Information zu verifizieren;
auf die Datenkomponente des inaktiven Zugriffssteuerungsclienten zuzugreifen; und
die Datenkomponente zu dem Anforderer zurückzugeben.

Es folgen 7 Seiten Zeichnungen

Anhängende Zeichnungen

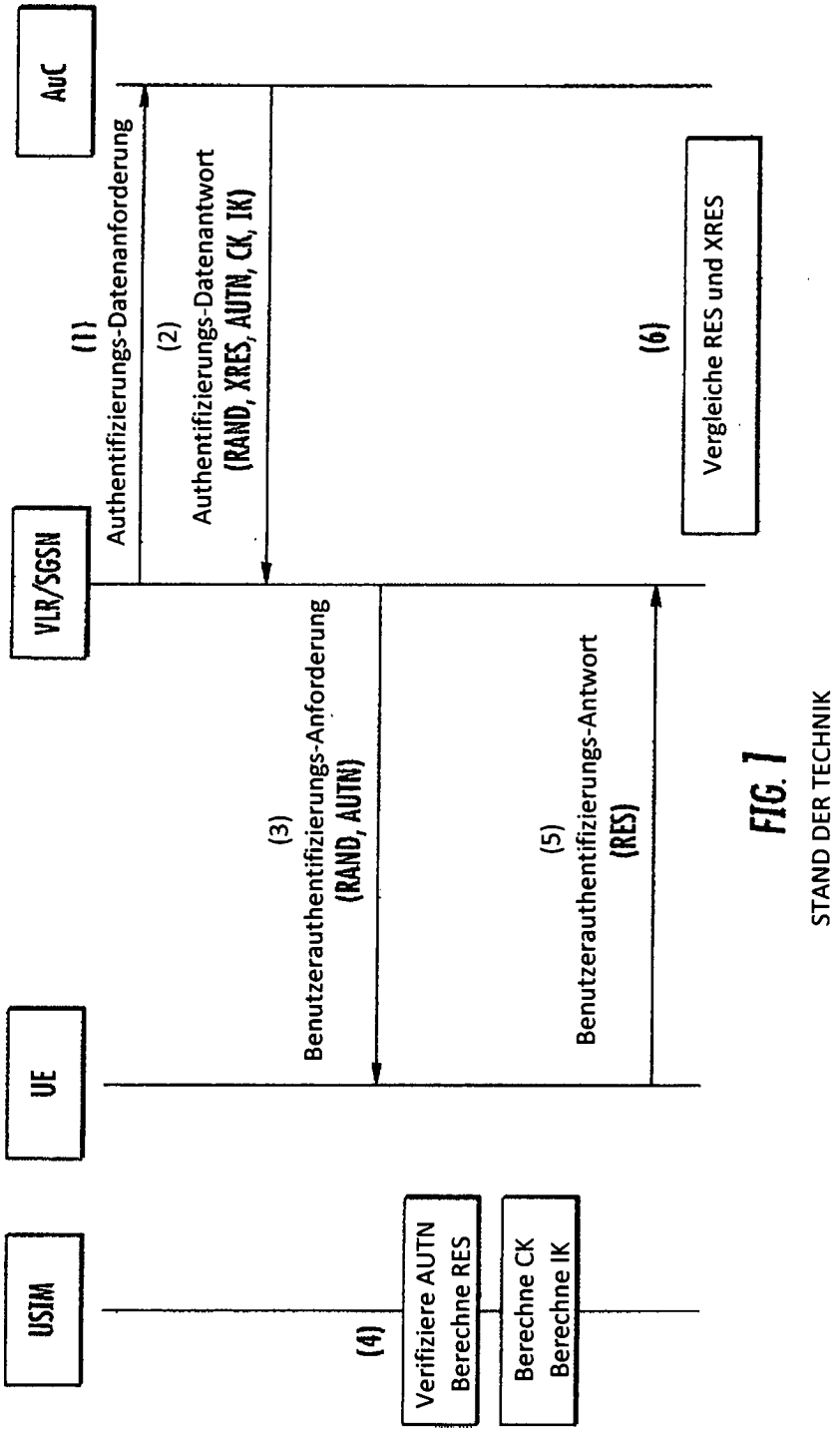


FIG. 1
STAND DER TECHNIK

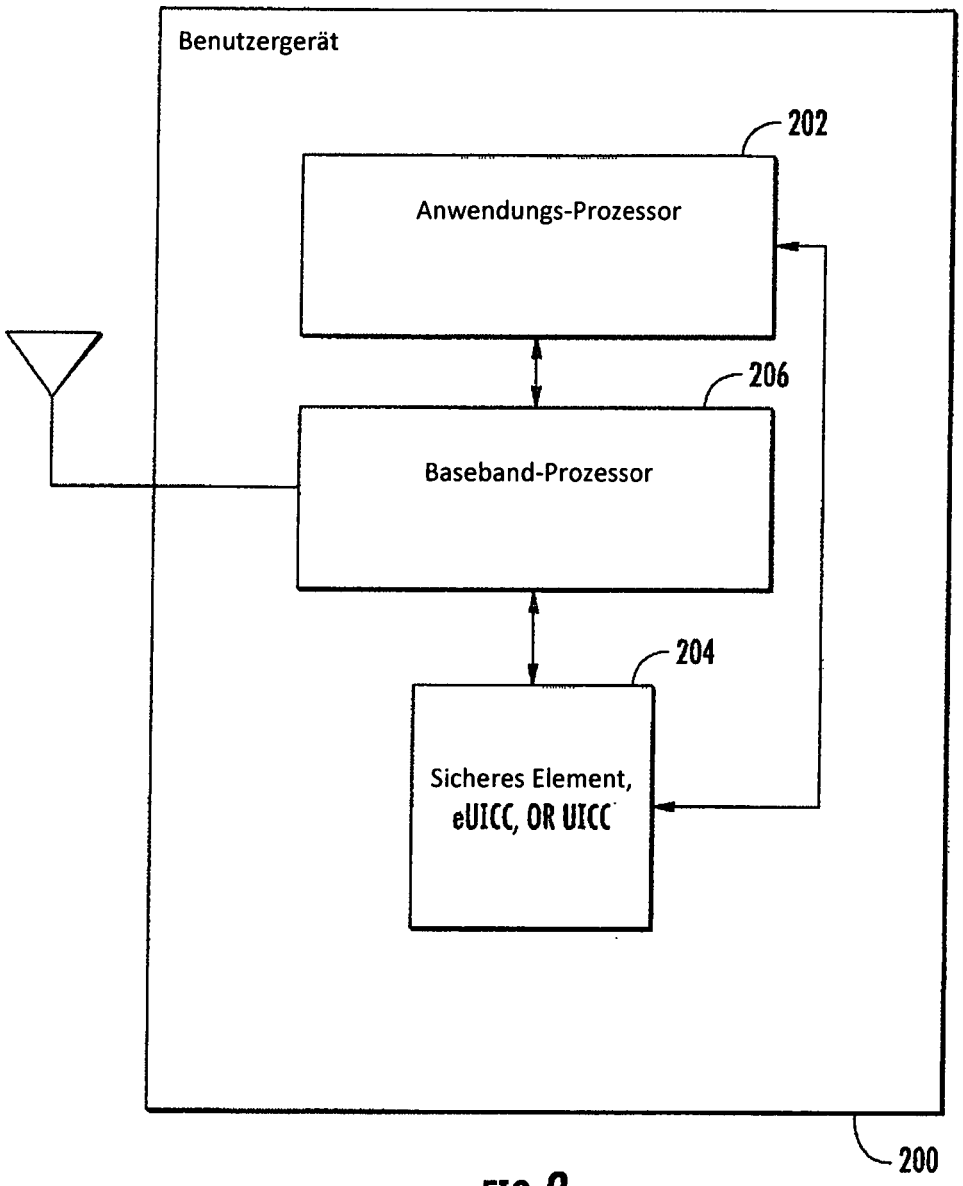

Benutzergerät
202
Anwendungs-Prozessor
206
Baseband-Prozessor
204
Sicheres Element,
eUICC, OR UICC
200

FIG. 2

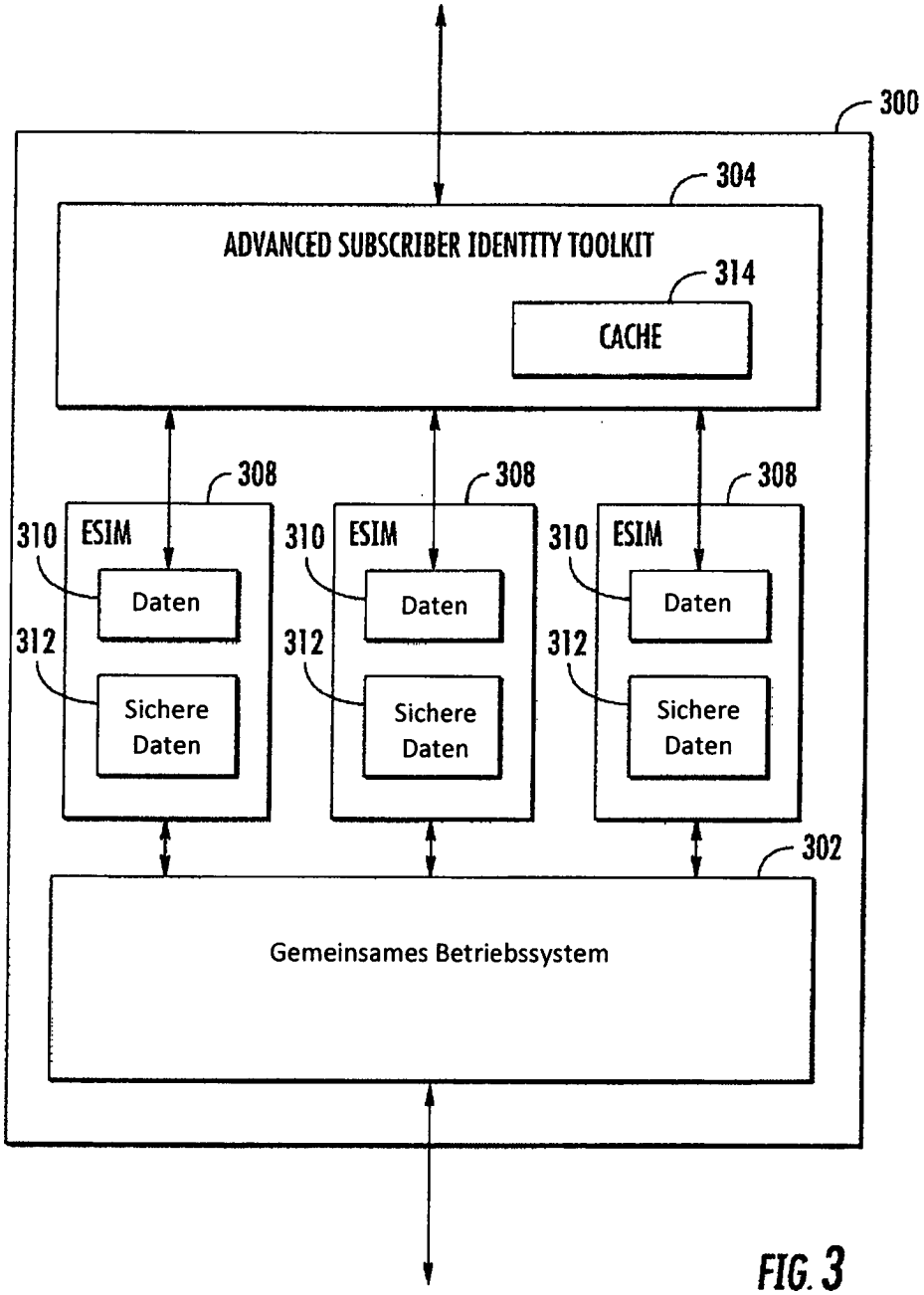

300
304
ADVANCED SUBSCRIBER IDENTITY TOOLKIT
314
CACHE
308
308
308
310
ESIM
310
ESIM
310
ESIM
Daten
Daten
Daten
312
312
312
Sichere Daten
Sichere Daten
Sichere Daten
302
Gemeinsames Betriebssystem

FIG. 3

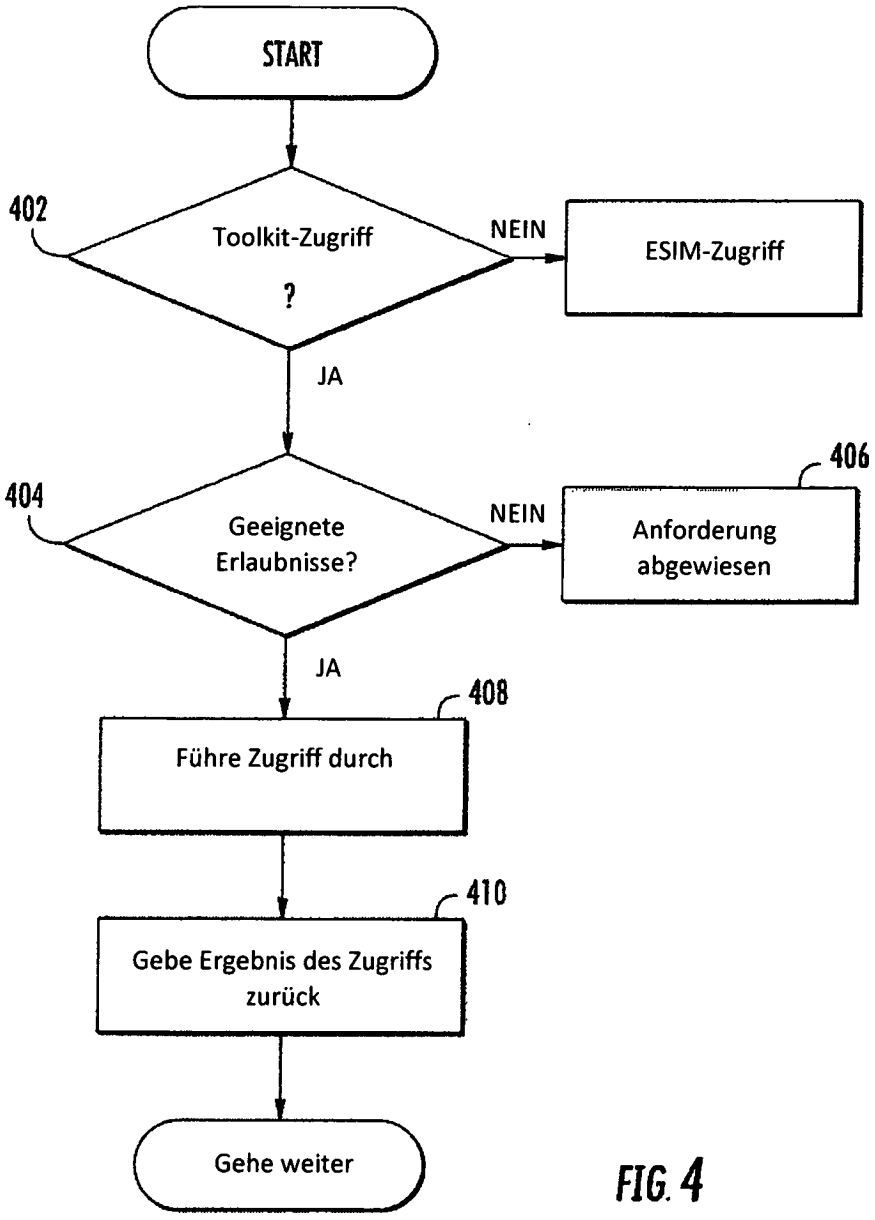

START
402
Toolkit-Zugriff ?
NEIN
ESIM-Zugriff
JA
404
Geeignete Erlaubnisse?
NEIN
406
Anforderung abgewiesen
JA
408
Führe Zugriff durch
410
Gebe Ergebnis des Zugriffs zurück
Gehe weiter

FIG. 4

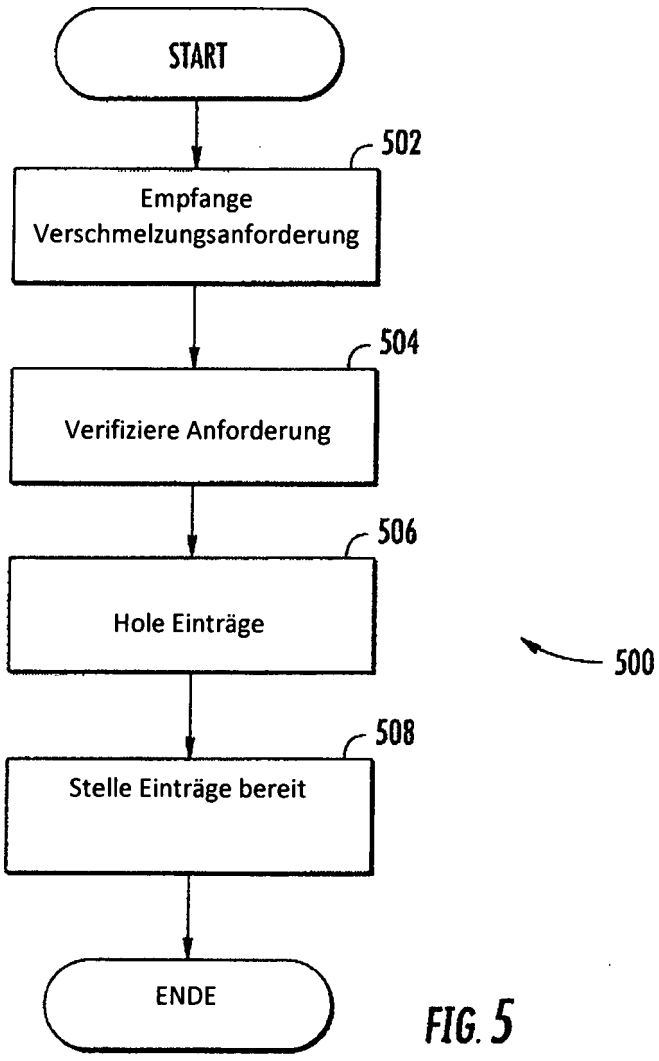

START
502
Empfange Verschmelzungsanforderung
504
Verifiziere Anforderung
506
Hole Einträge
500
508
Stelle Einträge bereit
ENDE

FIG. 5

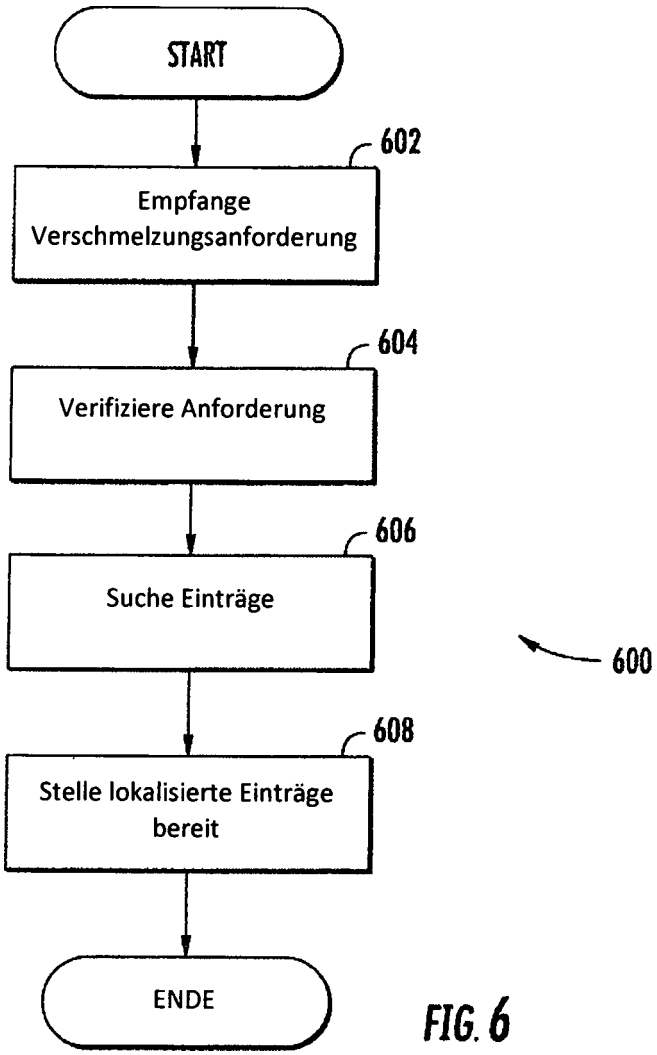

START
602
Empfange Verschmelzungsanforderung
604
Verifiziere Anforderung
606
Suche Einträge
600
608
Stelle lokalisierte Einträge bereit
ENDE

FIG. 6

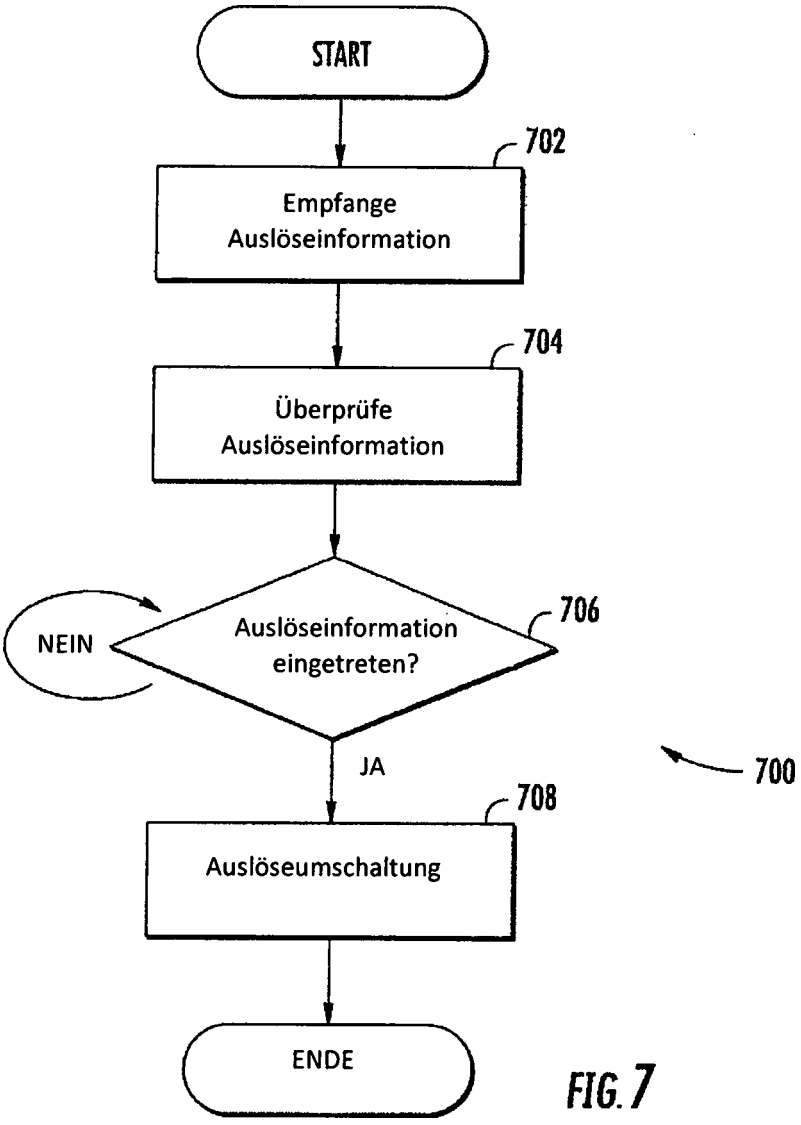

START
702
Empfange Auslöseinformation
704
Überprüfe Auslöseinformation
706
Auslöseinformation eingetreten?
NEIN
JA
700
708
Auslöseumschaltung
ENDE

FIG. 7