(19) Deutsches Patent- und Markenamt

(10) **DE 10 2017 008 045 A1** 2019.02.28

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2017 008 045.3**
(22) Anmeldetag: **25.08.2017**
(43) Offenlegungstag: **28.02.2019**

(51) Int Cl.: ***G06F 21/34*** (2013.01)
H04L 9/32 (2006.01)

(71) Anmelder:
Giesecke+Devrient Mobile Security GmbH, 81677 München, DE

(72) Erfinder:
Kondejkar, Pallavi, Pune, IN

(56) Ermittelter Stand der Technik:

US	**8 276 816**	**B2**
US	**2012 / 0 018 512**	**A1**
US	**2015 / 0 106 221**	**A1**
US	**2017 / 0 232 300**	**A1**

AWS IoT, Developer Guide, 22. Juni 2017

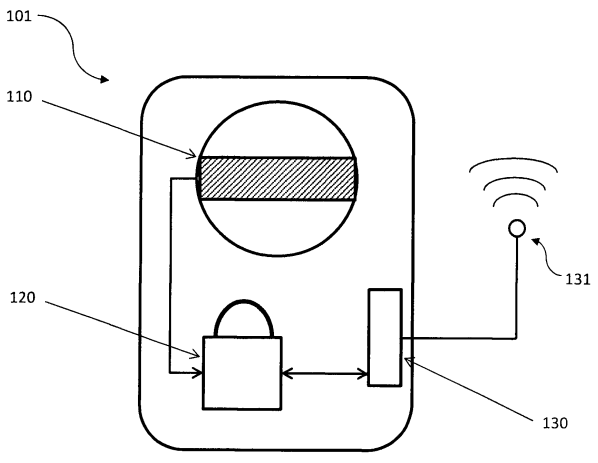
Melanie Swan: „Sensor Mania! The Internet of Things, Wearable Computing, Objecti ve Metrics, and the Quantified Self 2.0“, J. Sens. Actuator Netw. 2012, 1, 217-253; doi:10.3390/jsan1030217

Prüfungsantrag gemäß § 44 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **Vertrauenswürdiger Smart Button**

(57) Zusammenfassung: Die Erfindung betrifft einen Smart Button, der einen Sensor zur Interaktion mit der physischen Welt, eine Kommunikationsschnittstelle zur Kommunikation mit einem Server und ein Sicherheitselement, das eingerichtet ist, einen Auslöser von dem Sensor auszuwerten und eine vertrauenswürdige Anfrage für den Server zu generieren, umfasst. Der Smart Button ist eine Einzweckvorrichtung, welche eine vertrauenswürdige Anfrage über die Kommunikationsschnittstelle sendet, wenn die Auswertung des Auslösers anzeigt, dass eine Anfrage gesendet werden sollte.



Beschreibung

GEBIET DER ERFINDUNG

[0001] Die vorliegende Erfindung befasst sich mit dem wachsenden Bedarf für einfach zu verwendende Vorrichtungen, welche es einem Benutzer ermöglichen, eine Transaktion zu starten, während Vertrauen bewahrt wird. Insbesondere kann es wünschenswert sein, Transaktionen, wie eine Kaufanfrage, durch den einfachen Druck eines Knopfes durchzuführen, wobei der Beteiligte oder die Vorrichtung, an den bzw. die die Anfrage gerichtet ist, der Anfrage vertrauen kann.

HINTERGRUND

[0002] Vorrichtungen, welche bei Drücken eines Knopfes einem Server signalisieren, eine Transaktion zu starten, werden oft „Smart Buttons“ genannt, Beispiele. enthalten den Amazon Dash Button (https://en.wikipedia.org/wiki/Amazon_Dash), aber auch Flic, Cliki und NodOn NIU. Im Allgemeinen funktionieren diese Knöpfe dadurch, dass, wenn der Knopf gedrückt wird, eine Nachricht oder ein Paket mit einer Anfrage für eine Transaktion drahtlos gesendet wird. Solche Vorrichtungen vereinfachen das Starten oder Auslösen einer Transaktion, weil sie (verglichen mit einem PC oder Smartphone) in der Lage sind, eine Transaktion nur auszulösen, und keine ausgefeilte Benutzerschnittstelle aufweisen oder brauchen.

[0003] Im Falle des Amazon Dash, wird das Paket über WiFi (die IEEE 802.11) an einen Router und dann weiter an einen Server gesendet, wo das Paket als eine Anfrage von einem bestimmten Beteiligten interpretiert wird, ein bestimmtes Produkt zu kaufen. Der Server kann ein Amazon-Server sein, welcher die Anfrage einem Kundendatensatz zuordnet. Die Reaktion auf die Anfrage basiert darauf, dass der Knopf gedrückt wird, das heißt der Knopf ist einem Beteiligten und einem Produkt zugeordnet.

[0004] Als ein anderes Beispiel benutzt der NodOn NIU (www.amazon.com/NIU-Smart-Button-Android-NodOn/dp/B01HOOE60O) eine drahtlose Kommunikation über Bluetooth. Ein Knopfdruck sendet eine Nachricht oder ein Paket an ein Smartphone, wo dies als eine Anfrage interpretiert wird, eine vorausgewählte Aktion oder Transaktion durchzuführen. Der Knopfdruck kann auch codiert sein, sodass es verschiedene Aktionen gibt, die zum Beispiel einem einfachen Druck, einem doppelten Druck oder einem langen Druck zugeordnet sind. Das Smartphone agiert als ein Server, die Anfrage zu interpretieren und die gewünschten Folgeaktionen zu betreiben.

[0005] Eine minimalistische Schnittstelle zur einfachen Handhabung und geringe Kosten grenzen einen Smart Button ab. Es gibt typischerweise nur einen Sensor, welcher so einfach sein kann wie ein zu drückender Knopf oder ein zu berührender Fingerabdruckscanner oder dergleichen. Es kann keine Möglichkeit für den Smart Button geben, anzuzeigen, dass eine Anfrage ausgelöst worden ist, oder es kann ein einfacher Mechanismus, wie beispielsweise ein Aufleuchten eines Lichts oder ein akustisches Signal vorgesehen sein, um dem Benutzer Rückmeldung zu geben.

[0006] Der Vorteil eines Smart Button liegt in seiner Einfachheit. Im Falle des Amazon Dash genügt ein Druck des Knopfes, um die Kaufanfrage auszulösen, welche zur Lieferung des Produkts führt. Es gibt keine zusätzlichen Funktionalitäten, die eine Auswahl einer von vielen möglichen Funktionalitäten durch einen Benutzer erfordern. Der Smart Button kann als eine EinzweckVorrichtung angesehen werden, wobei der einzige Zweck darin liegt, eine Anfrage für eine Transaktion zu senden. Da die Schnittstelle so einfach ist, hat der Benutzer keine Auswahl zu treffen, wenn er den Smart Button benutzt. Ein Knopfdruck kann alles sein, was möglich ist.

[0007] Existierende vertrauenswürdige Rechnerumgebungen, wie sie beispielsweise in einem Smartphone gefunden werden können, sind schwer zugänglich. Ein PIN-Code oder eine andere Sicherheitsüberprüfung kann notwendig sein, um ein Smartphone zu entsperren, und es kann notwendig sein, durch mehrere Menüs zu gehen, um einen Kauf zu tätigen oder eine Transaktion anzufragen. Eine Transaktionskarte, wie beispielsweise eine EMV-kompatible Kreditkarte, muss mit einem Lesegerät verbunden werden, um funktionsbereit zu werden. Ein Computer mit einem Modul für eine vertrauenswürdige Plattform („Trusted Platform Module“, TPM) muss eingeschaltet werden und in Betrieb sein und kann zusätzliche Verbindungen, wie beispielsweise eine Energieversorgung erfordern, um betriebsfähig zu sein. Ein Smart Button ist einfach zu benutzen - in einem Ausführungsbeispiel ist eine Berührung eines Fingers ausreichend - und kann in der Lage sein, für eine lange Zeitspanne betriebsfähig zu sein, nur durch Verwendung der durch eine Batterie zugeführten Energie.

[0008] Es kann wünschenswert sein, die Person zu identifizieren, die den Knopf drückt, und sogar zu identifizieren, welcher Teil des Fingers oder Hand verwendet wird. Dies kann durch Benutzung von Fingerabdruckscannern erfolgen, welche für diesen Zweck verfügbar sind, z.B. www.fingerprints.com/technology/hardware/fpc1145. In einer Erweiterung zu dieser Idee, kann dieser gescannte Fingerabdruck verwendet werden, zu identifizieren, wessen Fingerabdruck und welcher Teil des Fingers benutzt wurde, siehe z.B. www.heise.de/newsticker/meldung/Tapdo-

Smart-Button-mit-integriertem-Fingerabdrucksensor-3639543 .html. Die gescannte Fingerabdruckinformation wird von dem Knopf an einen Server (wie beispielsweise ein Smartphone) drahtlos übertragen. Der Server analysiert dann die gescannte Information und ermittelt, welche Folgeaktionen (falls vorhanden) passend sind.

[0009] Es kann wünschenswert sein, das Vertrauensniveau im System zu erhöhen, besonders zwischen dem Knopf und dem Server. Es kann wünschenswert sein, dass der Server in der Lage ist, den Anfragen, die er von dem Knopf empfängt, zu vertrauen. Und es kann wünschenswert sein, dass die Information in der Anfrage (wie beispielsweise ein Fingerabdruckscan) verschlüsselt ist, sodass sie nur von dem Server, welcher sie empfängt, oder nur durch einen autorisierten Empfänger gelesen werden kann.

ZUSAMMENFASSUNG DER ERFINDUNG

[0010] Vertrauen kann durch Einbinden von Sicherheitsfähigkeiten in den Smart Button erreicht werden; gleichermaßen können die Anfragen von dem Knopf durch den Knopf verschlüsselt werden, bevor sie gesendet werden. In einem Ausführungsbeispiel kann der Knopf durch das Einbinden einer sicheren Verarbeitungsfähigkeit und sicheren Schlüsselspeicherfähigkeiten, welche in einem Ausführungsbeispiel in einem Sicherheitselement („Secure Element“) oder einer Sicherheits-Enklave („Secure Enclave“) sein können, ein vertrauenswürdiger Smart Button werden. Ein Sicherheitselement („Secure Element“, SE) kann in der Lage sein, einen Schlüssel auf eine Weise zu speichern, dass der Schlüssel außer mit einem enormen Rekonstruktionsaufwand („Reverse Engineering“) nicht zugänglich ist; gleichermaßen kann ein SE in der Lage sein, Verschlüsselung einer Nachricht, wie beispielsweise einer Anfrage, durchzuführen, ohne dass die Inhalte der Nachricht außerhalb des SE verfügbar sind. In einem Aspekt der Erfindung hält das SE in dem Knopf einen privaten Schlüssel bereit, welcher benutzt werden kann, die Nachricht zu signieren, bevor sie gesendet wird. In einem Aspekt verifiziert der Server, dass die Signatur der Anfrage mit der Signatur, die er von dem Knopf erwartet, übereinstimmt, und handelt entsprechend.

Figurenliste

Fig. 1 zeigt einen vertrauenswürdigen Smart Button.

Fig. 2 zeigt einen vertrauenswürdigen Smart Button, der drahtlos mit einem Server kommuniziert.

Fig. 3a, **Fig. 3b**, **Fig. 3c** zeigen die Betriebsphasen eines vertrauenswürdigen Smart Button.

DETAILLIERTE BESCHREIBUNG

[0011] Ein bevorzugtes Ausführungsbeispiel eines vertrauenswürdigen Smart Button ist in **Fig. 1** gezeigt. Der vertrauenswürdige Smart Button **101** umfasst einen Sensor, ein Sicherheitselement („Secure Element“) und eine Kommunikationsschnittstelle. Der Sensor **110** kann in einem bevorzugten Ausführungsbeispiel ein Fingerabdrucksensor sein. Der Fingerabdrucksensor kann aus Detektoren bestehen, welche einen Finger oder andere Teile einer Hand scannen und ein Bild in digitalem Format zur Verfügung stellen können. Der Sensor kann auch ein Iris-Scanner oder eine Kamera oder eine beliebige andere Art eines Sensors sein. Der Sensor kann mit einem Sicherheitselement **120** gekoppelt sein, welches die Information von dem Sensor empfängt. Die Information kann in einer digitalisierten Form vorliegen. In einem anderen Ausfiihrungsbeispiel kann der Sensor auch mit einem Verarbeitungselement (nicht gezeigt) gekoppelt sein, welches entweder das Sicherheitselement enthält oder mit dem Sicherheitselement verbunden ist.

[0012] Der Sensor kann durch Druck oder durch kapazitiven Kontakt zwischen dem Sensor und einem Finger ausgelöst werden. In einem Ausführungsbeispiel kann der Sensor einen Metallkontakt umfassen, um zu detektieren, dass der Sensor von einem Finger berührt worden ist, und um einen Fingerabdruckscan auszulösen.

[0013] Wenn der Sensor ausgelöst wird, wertet der Knopf das Sensorsignal aus und reagiert entsprechend. Die Auswertung kann in dem Sicherheitselement durchgeführt werden, oder kann in einem Verarbeitungselement (nicht gezeigt), welches in direkter Kommunikation mit dem Sicherheitselement steht, ausgewertet werden. In einem Ausführungsbeispiel kann der Impuls ein Fingerabdruck auf einem Fingerabdrucksensor sein. Der Fingerabdruck wird dem Sicherheitselement oder Verarbeitungselement zur Auswertung als ein Auslöser zur Verfügung gestellt. Falls das Sicherheitselement oder Verarbeitungselement feststellt, dass der Fingerabdruck zu einem Auslöser korrespondiert, welcher eine Anfrage aktivieren sollte, bewirkt das Sicherheitselement oder Verarbeitungselement, dass eine Nachricht oder eine Anfrage über die Kommunikationsschnittstelle **130** übertragen wird. Im Falle einer drahtlosen Schnittstelle wird die Anfrage über die Antenne **131** übertragen. Die Auswertung des Auslösers kann ein Auswerten des Fingerabdrucks als solches enthalten oder nicht; in einigen Ausführungsbeispielen kann es vorteilhaft sein, den „rohen“ Fingerabdruck für weitere spätere Auswertungen zu übertragen.

[0014] Das Sicherheitselement ist bei der Auswertung des Auslösers von dem Sensor involviert, um sicherzustellen, dass jede Anfrage, welche übertra-

gen wird, eine vertrauenswürdige Anfrage sein kann. Das direkte Koppeln von Sensor zu Sicherheitselement zu Kommunikationsschnittstelle erlaubt einen vertrauenswürdigen Betrieb mit minimalem Energieverbrauch.

[0015] Der Knopf kann ein Signalelement (nicht gezeigt) aufweisen oder nicht, wie beispielsweise ein Licht oder eine akustische Vorrichtung, um dem Benutzer optische oder akustische Rückmeldung zu geben, dass der Sensor ausgelöst worden ist oder eine Transaktion angefragt wurde.

[0016] Das Sicherheitselement **120** kann einen oder mehrere Schlüssel zur Verwendung beim Verschlüsseln und/oder Signieren von Anfragen enthalten. Ein Schlüssel kann ein privater Schlüssel zur Verwendung in einer asymmetrischen Kryptographie (Public-Key-Kryptographie) sein. Der korrespondierende öffentliche Schlüssel kann einem Server zur Verfügung gestellt werden, wie nachfolgend beschrieben. Ein Schlüssel kann zur Verwendung beim Kodieren einer Anfrage oder Nachricht ein symmetrischer Schlüssel sein. Die Anfrage kann Sensorinformation enthalten, welche unter Verwendung des symmetrischen Schlüssels codiert werden kann, bevor sie übertragen wird. Die Sensorinformation kann ein Scan eines Fingerabdrucks sein. Der symmetrische Schlüssel kann mit einem Server unter Verwendung asymmetrischer Kryptographie, wie beispielsweise Public-Key-Kryptographie, ausgetauscht worden sein. Der symmetrische Schlüssel kann eine begrenzte Gültigkeitsdauer aufweisen, bevor er ersetzt wird, und kann ein Sitzungsschlüssel sein. In einem Ausführungsbeispiel kann der Sensor einen Fingerabdruckscan zur Verfügung stellen, welcher digital an das Sicherheitselement übertragen wird und dann im Sicherheitselement unter Verwendung eines symmetrischen Schlüssels verschlüsselt wird. Die verschlüsselten Daten werden dann der Kommunikationsschnittstelle **130** zur Übertragung zur Verfügung gestellt.

[0017] In einem Ausführungsbeispiel kann das SE oder der Prozessor die Information von dem Sensor auswerten und feststellen, welcher Beteiligte die Anfrage macht. Der Beteiligte, der den Sensor auslöst, kann eine Person sein, sogar ein Kind oder ein Tier oder ein Objekt. In einem Ausführungsbeispiel kann das SE oder der Prozessor einen Fingerabdruckscan auswerten und feststellen, wessen Fingerabdruck gescannt wurde. Die Identifikation des Beteiligten, der den Sensor auslöst, kann an den Server übertragen werden; diese Identifikation kann verschlüsselt werden, bevor sie an den Server gesendet wird. In einem anderen Ausführungsbeispiel kann das SE oder der Prozessor die Information von dem Sensor über die Kommunikationsschnittstelle an den Server übertragen. In einem Ausführungsbeispiel kann die Information von dem Sensor verschlüsselt werden, bevor sie übertragen wird.

[0018] Der vertrauenswürdige Smart Button kommuniziert mit einem Server, wie in **Fig. 2** gezeigt. In einem bevorzugten Ausführungsbeispiel kommuniziert der vertrauenswürdige Smart Button **201** über eine drahtlose Verbindung mit einem Server **250**. Die Kommunikation kann auch über eine optische Verbindung (nicht gezeigt) oder über ein anderes Medium, wie beispielsweise ein Kabel (nicht gezeigt), stattfinden. Die Verbindung kann direkt sein, wie es der Fall in **Fig. 2** wäre, oder durch einen Router oder andere Vermittler gehen.

[0019] Der Server **250** kann an einem entfernten Ort, wie beispielsweise ein Amazon-Server, sein. Alternativ kann der Server lokal sein und kann ein Smartphone sein, das eingerichtet ist, Anfragen von dem Knopf zu empfangen. Der Server ist eingerichtet, eine Anfrage von dem Knopf zu empfangen, wenn der Knopf aufgrund des ausgelösten Sensors eine Anfragenachricht sendet.

[0020] Der Smart Button und der Server können initial durch Austauschen von Schlüsseln eine vertrauenswürdige Beziehung einrichten. Der Server kann dem Knopf einen öffentlichen Schlüssel zur Verfügung stellen, und der Knopf kann dem Server einen öffentlichen Schlüssel zur Verfügung stellen. Der Knopf und der Server können auch oder alternativ symmetrische Schlüssel austauschen. In einem Ausführungsbeispiel kann der Knopf hybride Verschlüsselung verwenden, wo asymmetrische Verschlüsselung für Austausche geringer Intensität, wie beispielsweise Austauschen von symmetrischen Schlüsseln, verwendet wird, und symmetrische Verschlüsselung für Austausche hoher Intensität, wie beispielsweise eine Transaktionsanfrage, verwendet wird. Der Knopf kann einen Schlüssel oder Schlüssel im Sicherheitselement speichern. Der Austausch von Schlüsseln kann unter Verwendung eines anderen Kommunikationsmediums stattfinden, als das verwendet wird, um die Nachrichten mit Anfragen zu senden. Der Schlüssel oder die Schlüssel für den Knopf kann bzw. können während der Herstellung oder während eines Personalisierungsschritts oder in einer Einrichtungsphase, wo der Knopf zur Verwendung vorbereitet wird, dem Knopf zur Verfügung gestellt oder in ihn eingegeben werden. Dies würde zum Beispiel ein Bereitstellen über die Luft („over-the-air“, OTA) enthalten.

[0021] In einem Ausführungsbeispiel kann der Knopf mit einem Server eine vertrauenswürdige Beziehung über eine Interaktion mit einem Smartphone oder anderen Prozessor, welcher nicht der Server ist, einrichten. Das Smartphone kann eine Applikation („App“) unterstützen, welche die Konfiguration der passenden Antwort auf eine Anfragenachricht ermöglicht.

Der Knopf kann sich mit dem Smartphone drahtlos oder optisch oder mittels Ultraschall verbinden, und das Smartphone kann als ein Router oder eine Bridge zwischen dem Knopf und dem Server dienen. Während des Einrichtens kann ein initialer Schlüsselaustausch über das Smartphone stattfinden.

[0022] In einem anderen Ausführungsbeispiel kann der Server ein Smartphone sein, und der Knopf kann unter Verwendung einer drahtlosen oder optischen oder drahtgebundenen Verbindung oder einer beliebigen Kombination von diesen eine vertrauenswürdige Beziehung mit dem Server einrichten. Der Server und der Knopf können Schlüssel direkt austauschen oder sie können sich auf einen vertrauenswürdigen Dritten als Vermittler verlassen. Insbesondere können sie sich auf eine Fremdzertifizierungsstelle verlassen, um gegenseitiges Vertrauen herzustellen.

[0023] Der Knopf kann während der Einrichtungsphase nur Kommunikation mit einem Kommunikationsmedium kurzer Reichweite, wie beispielsweise Bluetooth oder optische Verbindungen, akzeptieren. Der Knopf kann in eine Einrichtungsphase eintreten, zum Beispiel falls der Sensor einen bestimmten Auslöser, wie beispielsweise einen sehr langen Knopfdruck, detektiert. In einem anderen Ausführungsbeispiel kann der Knopf in eine Einrichtungsphase eintreten, wenn er eine bestimmte Nachricht über ein Kommunikationsmedium empfängt.

[0024] Die verschiedenen Betriebsphasen eines Ausführungsbeispiels eines vertrauenswürdigen Smart Button sind in den **Fig. 3a**, **Fig. 3b**, **Fig. 3c** gezeigt.

[0025] **Fig. 3a** zeigt eine Bereitstellungsphase, während welcher ein asymmetrisches Schlüsselpaar öffentlicher/privater Schlüssel dem Sicherheitselement des Smart Button zur Verfügung gestellt wird. Der private Schlüssel wird im Sicherheitselement behalten und der öffentliche Schlüssel kann anderen Aktoren in einem System, wie beispielsweise einem Server, zur Verfügung gestellt werden. Das Bereitstellen kann während der Herstellung oder während einer Personalisierung des Knopfes oder zu irgendeinem anderen Zeitpunkt stattfinden, wo es möglich ist, sicherzustellen, dass der private Schlüssel nicht gefährdet wird.

[0026] **Fig. 3b** zeigt eine Einrichtungsphase. Während der Einrichtungsphase kann der Smart Button konfiguriert werden. In einem Ausführungsbeispiel, gezeigt in **Fig. 3b**, tritt der Knopf in Schritt **321** in einen Einrichtungs-Betriebsmodus ein. Ein Kommunikationskanal zwischen dem Knopf und einem Server wird in Schritt **322** hergestellt. In einem Ausführungsbeispiel kann dies ein Kanal sein, der eine andere Technologie als der Kanal verwendet, der für die Kommunikationsanfrage in **Fig. 3c** verwendet wird, zum Beispiel unter Verwendung von Bluetooth anstatt Wi-Fi. Der öffentliche Schlüssel des Knopfes kann in Schritt **322** einem Server oder ein Smartphone oder irgendeinem anderen Prozessor zur Verfügung gestellt werden. Der Server verschlüsselt einen symmetrischen Schlüssel mit dem öffentlichen Schlüssel des Knopfes und stellt ihn in Schritt **323** dem Knopf zur Verfügung. Der verschlüsselte symmetrische Schlüssel kann in dem Sicherheitselement unter Verwendung des privaten Schlüssels auch entschlüsselt werden. Ein Beispiel eines symmetrischen Schlüssels, welcher für ein Ausführungsbeispiel verwendet werden könnte, ist AES. Der Server stellt in Schritt **324** dann die Adresse zur Verfügung, an welche Transaktionsanfragen gesendet werden sollten (derselbe oder ein anderer Server). Diese Information kann mit dem symmetrischen Schlüssel codiert werden, sodass sie geheim ist. In anderen Ausführungsbeispielen kann Schritt **324** parallel zu oder vor Schritt **323** stattfinden.

[0027] Die während der Einrichtungsphase zur Verfügung gestellte Konfiguration kann die Adressinformation enthalten, die notwendig ist, Anfragen an den Server entweder direkt oder indirekt über Gateways oder Router zu senden. Die Konfiguration kann eine Auswahl enthalten, welche Information in der Anfrage zur Verfügung gestellt wird. In einem Ausführungsbeispiel kann der Knopf mit der IP-Adresse eines Servers konfiguriert werden und kann konfiguriert werden, den Scan von dem Fingerabdrucksensor zu übertragen, immer wenn der Knopf gedrückt wird.

[0028] In die Einrichtungsphase kann automatisch eingetreten werden, wenn der Knopf zum ersten Mal verwendet wird, oder es kann basierend auf bestimmten Bedingungen oder Signalen in sie eingetreten werden. In die Einrichtungsphase kann auch wieder eingetreten werden, um den Knopf wieder zu konfigurieren. Konfiguration des Knopfes kann unter Verwendung eines Kommunikationskanals oder eines separaten Kommunikationskanals wie oben beschrieben erfolgen, oder sie kann unter Verwendung anderer Verfahren erfolgen, zum Beispiel mit entfernbaren Aufklebern, welche zu dem bestimmten zu bestellenden Produkt korrespondieren. Die Aufkleber können eine maschinenlesbare Komponente umfassen, um es dem Knopf zu ermöglichen, seine neue Konfiguration festzustellen.

[0029] Sobald die für die Einrichtung notwendigen Vorgänge abgeschlossen worden sind, verlässt der Knopf den Einrichtungsmodus bei Schritt **325**.

[0030] **Fig. 3c** zeigt den Betrieb eines Ausführungsbeispiels des Smart Button mit einem Fingerabdruckscanner, wenn der Sensor ausgelöst wird. In Schritt **331** wird der Sensor ausgelöst, zum Beispiel durch eine Berührung eines Knopfes oder Kontakt mit dem Fingerabdruckscanner. In Schritt **332** wird ein Scan

des Fingerabdrucks dem Sicherheitselement zur Verfügung gestellt. Alternativ kann der Scan einem Prozessor (nicht gezeigt) zur Verfügung gestellt werden, welcher mit dem Sicherheitselement zusammenarbeitet. In diesem Ausführungsbeispiel wird der Scan von dem Sicherheitselement unter Verwendung des symmetrischen Schlüssels aus **Fig. 3b** in Schritt **333** verschlüsselt. In anderen Ausführungsbeispielen kann der Scan unter Verwendung des privaten Schlüssels des Knopfes signiert werden.

[0031] Während des Prozesses des Vorbereitens der Nachricht in Schritt **333** kann ein Ereigniszähler oder ein Nonce hinzugefügt werden, zum Beispiel um Wiederholungsangriffe zu unterbinden. Es kann wünschenswert sein, dass ein Lauscher die Transaktionsanfrage nicht replizieren kann und dadurch mehrfache Transaktionen starten kann.

[0032] In Schritt **334** wird der verschlüsselte Scan vom Sicherheitselement an die Kommunikationsschnittstelle weitergeleitet. In anderen Ausführungsbeispielen kann der Scan nicht verschlüsselt sein und kann signiert sein oder nicht und kann einen Zähler oder Nonce enthalten oder nicht, um gegen Wiederholungsangriffe zu schützen. In anderen Ausführungsbeispielen können die Sensordaten bereits ausgewertet worden sein, und zum Beispiel der Fingerabdruck oder andere Sensordaten können einem bestimmten Individuum zugeordnet sein, und nur die Identifikation dieses Individuums kann dann der Kommunikationsschnittstelle zur Verfügung gestellt werden.

[0033] In Schritt **335** wird die aus Schritt **334** resultierende vertrauenswürdige Transaktionsanfrage an ihr Ziel weitergeleitet, entweder mit einer direkten Kommunikationsverbindung oder über einen Router oder ein Gateway. In einem Ausführungsbeispiel kann die Kommunikationsschnittstelle Bluetooth verwenden, um die vertrauenswürdige Anfrage direkt an ein Smartphone oder anderen Computer, welcher die Anfrage empfängt, zu übertragen. In einem anderen Ausführungsbeispiel kann die Kommunikationsschnittstelle WiFi verwenden, um die Anfrage an einen Wi-Fi-Router zu übertragen, um an einen Server weitergeleitet zu werden.

[0034] In der vorhergehenden Beschreibung wurden vielfältige bevorzugte Ausführungsbeispiele mit Bezug auf die begleitenden Zeichnungen beschrieben. Die vorstehende Beschreibung zusammen mit ihren zugehörigen Ausführungsbeispielen wurde nur zum Zwecke der Veranschaulichung wiedergegeben. Sie ist nicht erschöpfend und beschränkt die Erfindung nicht auf die offenbarte präzise Form. Zum Beispiel müssen Schritte nicht in der gleichen Reihenfolge, wie wiedergeben, durchgeführt werden; gleichermaßen können Schritte weggelassen, wiederholt oder kombiniert werden, wie notwendig, um die gleichen Ziele zu erreichen.

[0035] Ein Server wird als eine entfernte Rechnerquelle vorgestellt, welche als eine spezielle Entität organisiert sein kann, oder eine dezentrale Quelle, wie beispielsweise die „Cloud“, sein kann, welche über das Internet oder andere Netzwerke zugänglich ist.

[0036] Bezüglich der Verwendung hier im Wesentlichen jedes Plural- und/oder Singular-Begriffs kann ein Fachmann vom Plural zum Singular und/oder vom Singular zum Plural übersetzen, wie es durch den Kontext und/oder die Anwendung angemessen ist. Die vielfältigen Singular-/Plural-Permutationen können der Klarheit halber hier ausdrücklich dargelegt sein.

[0037] Die vorliegende Erfindung ist nicht auf die Ausführungsbeispiele beschränkt, die oben als Beispiele genommen wurden. Variationen und Modifikationen können durch einen Fachmann bewerkstelligt werden, und andere Ausführungsbeispiele der vorliegenden Erfindung sind einfach vorstellbar, ohne vom Umfang dieser Erfindung, wie in den Ansprüchen definiert, abzuweichen.

Patentansprüche

1. Smart Button, umfassend:
- einen Sensor zur Interaktion mit der physischen Welt,
- eine Kommunikationsschnittstelle zur Kommunikation mit einem Server, und
- ein Sicherheitselement, das eingerichtet ist,
- einen Auslöser von dem Sensor auszuwerten und
- eine vertrauenswürdige Anfrage für den Server zu generieren, wobei der Smart Button eine Einzweckvorrichtung ist, welche eine vertrauenswürdige Anfrage über die Kommunikationsschnittstelle sendet, wenn die Auswertung des Auslösers anzeigt, dass eine Anfrage gesendet werden sollte.

2. Smart Button nach Anspruch 1, wobei der Smart Button eingerichtet ist, sodass der Sensor dem Sicherheitselement einen Auslöser gibt, eine vertrauenswürdige Anfrage für den Server zu generieren, wobei die Anfrage dann über die Kommunikationsschnittstelle gesendet wird.

3. Smart Button nach einem der vorhergehenden Ansprüche, wobei der Sensor ein Fingerabdrucksensor ist.

4. Smart Button nach einem der vorhergehenden Ansprüche, wobei die Kommunikationsschnittstelle eine drahtlose Kommunikationsschnittstelle ist.

5. Smart Button nach Anspruch 4, wobei die drahtlose Kommunikationsschnittstelle Bluetooth oder Wi-Fi (IEEE 802.11) verwendet.

6. Smart Button nach einem der vorhergehenden Ansprüche, wobei das Sicherheitselement Nutzdaten mit symmetrischer Verschlüsselung verschlüsselt.

7. Smart Button nach Anspruch 6, wobei die symmetrische Verschlüsselung dem AES-Standard folgt.

8. Smart Button nach einem der vorhergehenden Ansprüche, wobei das Sicherheitselement einen privaten Schlüssel für asymmetrische Verschlüsselung besitzt.

9. Smart Button nach einem der vorhergehenden Ansprüche, wobei das Sicherheitselement eine hybride Verschlüsselung verwendet, um eine vertrauenswürdige Kommunikation herzustellen.

10. Smart Button nach Anspruch 9, welcher ein Signalelement, so wie ein Licht oder eine akustische Vorrichtung umfasst.

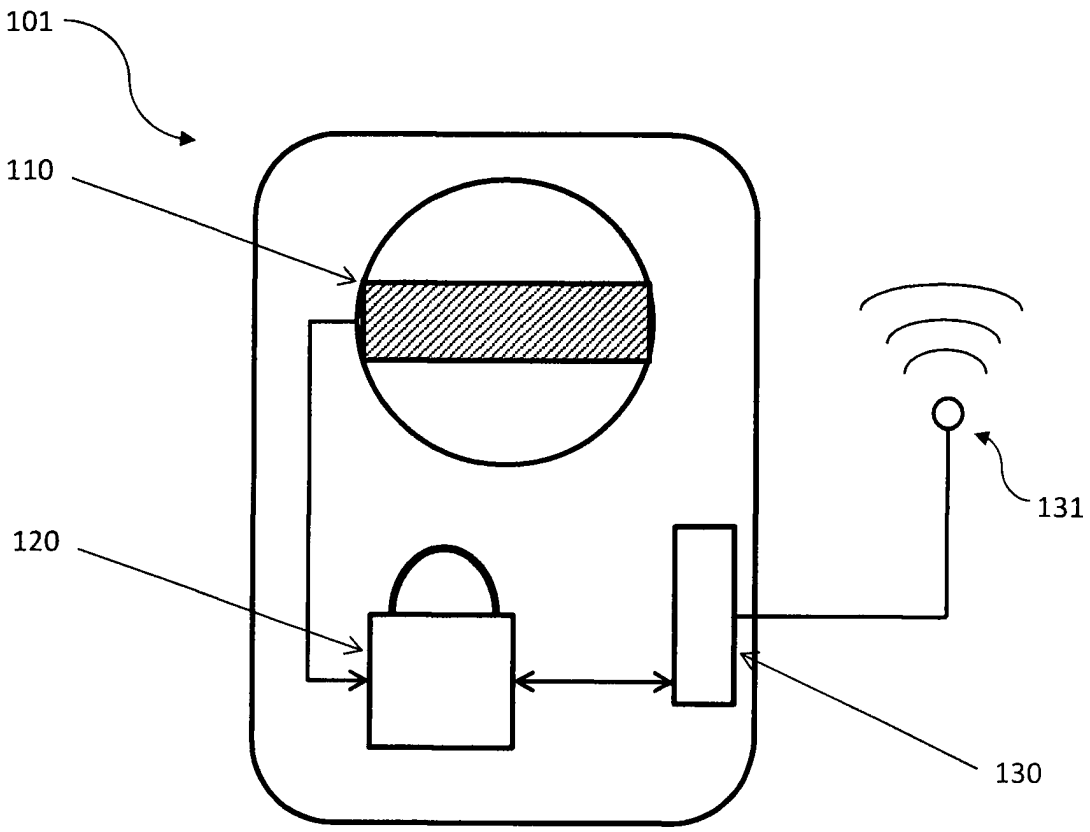
11. Verfahren zum Betreiben eines Smart Button, umfassend
- Empfangen eines Auslösers von zumindest einem Sensor zur Interaktion mit der physischen Welt,
- Auswerten des Auslösers und
- Senden einer vertrauenswürdigen Anfrage an einen Server, wenn die Auswertung anzeigt, dass eine Anfrage gesendet werden sollte.

12. Verfahren nach Anspruch 11, wobei die vertrauenswürdige Anfrage signiert ist, um Vertrauen herzustellen.

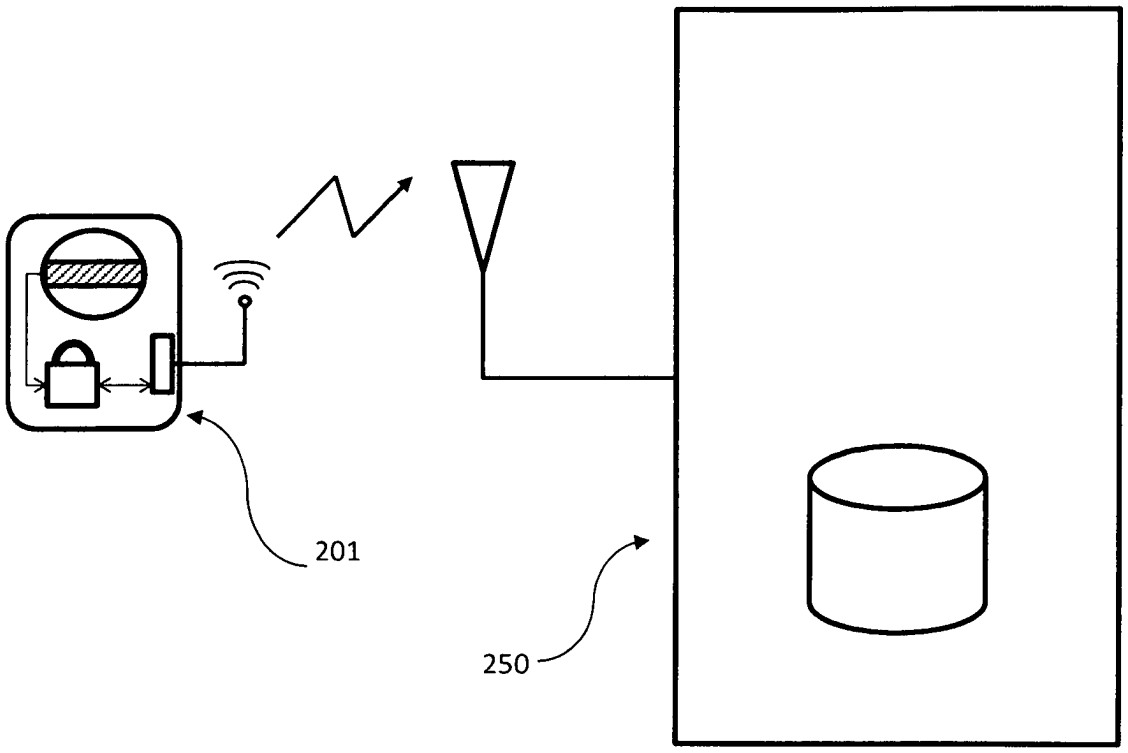
13. Verfahren nach Anspruch 11 oder 12, wobei die vertrauenswürdige Anfrage unter Verwendung von zuvor ausgetauschten Schlüsseln verschlüsselt ist.

Es folgen 3 Seiten Zeichnungen

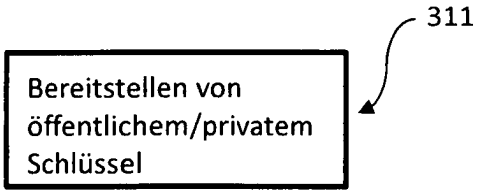
Anhängende Zeichnungen



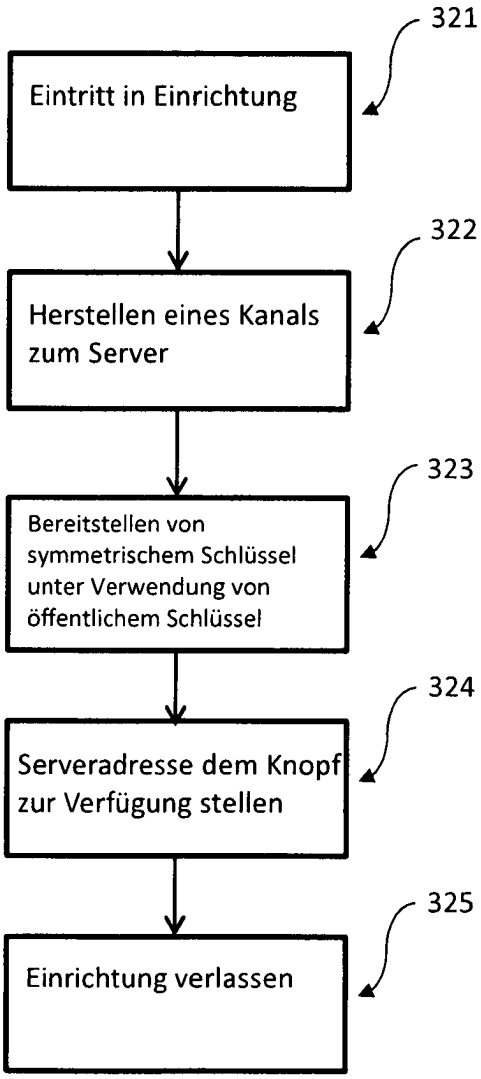
Figur 1



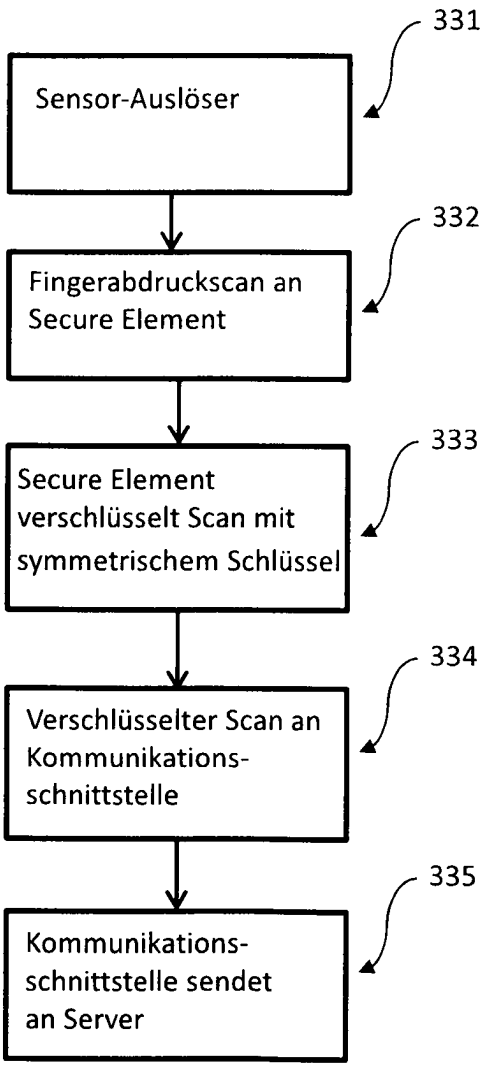
Figur 2



Figur 3a



Figur 3b



Figur 3c