(19) LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Économie

(11) N° de publication : **LU103080**

(12) **BREVET D'INVENTION** **B1**

(21) N° de dépôt: LU103080

(51) Int. Cl.:
G06F 21/60, G06F 21/82

(22) Date de dépôt: 28/02/2023

(30) Priorité:

(43) Date de mise à disposition du public: 28/08/2024

(47) Date de délivrance: 28/08/2024

(73) Titulaire(s):
KRALOS GMBH – 31303 Burgdorf (Allemagne)

(72) Inventeur(s):
GREIWE Christian Clemens – Allemagne, KLEIN Carsten – Allemagne

(74) Mandataire(s):
WHITE IP Patentanwaltskanzlei – 01097 Dresden (Allemagne)

(54) **VERFAHREN ZUR AUSGABE UND KOMMUNIKATION SENSIBLER VERSCHLÜSSELTER DATEN.**

(57) Die vorliegende Erfindung betrifft ein computerimplementiertes Verfahren zum Ausgeben und Kommunizieren verschlüsselter elektronischer Daten, sowie ein System, eine sekundäre Ausgabeeinheit und zwei Computerprogrammprodukte zur Implementierung des Verfahrens, welche der Ausgabe und Kommunikation sensibler verschlüsselter digitaler Daten dienen. Mit der vorliegenden Erfindung soll eine sekundäre Ausgabeeinheit zusätzlich zu einem existierenden Endgerät, der primären Ausgabeeinheit, zur Kommunikation bereitgestellt werden, mithilfe dessen Privatsphäre und Integrität von Nachrichtenkommunikation gewährleistet werden kann, auch unter Annahme einer unsicheren oder infizierten primären Ausgabeeinheit. Vorteilhaft wird dies mittels eines mehrschrittigen Verfahrens gelöst, wobei eine verschlüsselte Nachricht auf der primären Ausgabeeinheit gekennzeichnet, mittels einer unidirektionalen Datenübertragungstechnologie an die sekundäre Ausgabeeinheit gesendet, dort entschlüsselt und angezeigt wird. Mithilfe der sekundären Ausgabeeinheit kann eine andere Nachricht eingegeben, verschlüsselt und mittels einer unidirektionalen Ausgangsverbindung zurück an die primäre Ausgabeeinheit gesendet werden, von wo sie versendet werden kann.

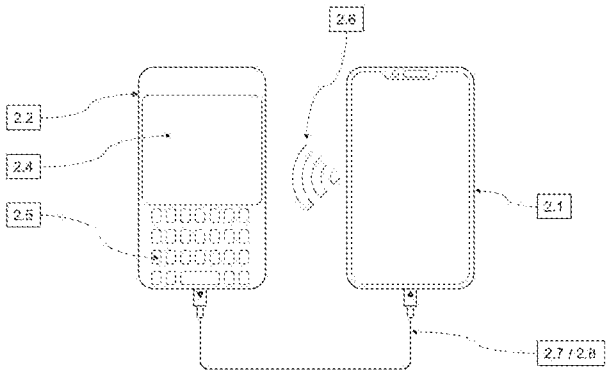

Fig. 2

VERFAHREN ZUR AUSGABE UND KOMMUNIKATION SENSIBLER VERSCHLÜSSELTER DATEN

LU103080

TECHNISCHES GEBIET

Die vorliegende Erfindung betrifft ein computerimplementiertes Verfahren gemäß dem Schutzanspruch 1, sowie ein System, eine sekundäre Ausgabeeinheit und zwei Computerprogrammprodukte zur Implementierung des Verfahrens, welche der Ausgabe und Kommunikation sensibler verschlüsselter digitaler Daten dienen. Mit der vorliegenden Erfindung soll eine sekundäre Ausgabeeinheit zusätzlich zu einer existierenden primären Ausgabeeinheit zur Kommunikation bereitgestellt werden, mithilfe dessen Privatsphäre und Integrität von Nachrichtenkommunikation gewährleistet werden kann, auch unter Annahme einer unsicheren oder infizierten primären Ausgabeeinheit.

STAND DER TECHNIK

Mit der zunehmenden, branchenübergreifenden Digitalisierung werden Nachrichteninformationen bevorzugt digital zwischen verschiedenen Endgeräten versendet. Durch das ständige Wachstum des Internets und die Verbreitung von persönlichen Daten ist es wichtiger denn je, die Sicherheit unserer Daten zu gewährleisten. Datenlecks und Cyberangriffe können schwerwiegende Folgen haben, von finanziellen Verlusten über den Eingriff in die individuelle Privatsphäre bis hin zu Reputationsschäden. Für bestimmte Branchen, Berufsgruppen und Nachrichtenarten muss beim Austausch von Nachrichten eine besonders hohe Anforderung an die Datensicherheit gestellt werden. Unter anderem Politiker, Journalisten, sowie Menschen, welche beruflich im Bereich der Intellectual Property oder bei Behörden arbeiten, kommunizieren regelmäßig datenschutztechnisch sensible Nachrichten auf digitale Weise. Für diese sensiblen Daten in digitaler Form muss ein besonders hohes Maß an IT-Sicherheit sichergestellt sein.

Für digitale Kommunikation werden als Endgeräte in der Regel PCs und besonders bevorzugt Smartphones verwendet. Die Daten werden bevorzugt über das Internet als Netzwerk übertragen werden. Ein Netzwerk, bei dem man davon ausgehen muss, dass ein potenzieller Angreifer in diesem Netzwerk Zugriff auf einen anderen Computer hat, sodass ein Angreifer beliebige Daten über das Netzwerk senden und abfangen kann, gilt als unsicher. Insbesondere das Internet gilt als unsicheres Netzwerk.

Um bei einer Datenübertragung im Internet Manipulationssicherheit bzw. Integrität zu gewährleisten, können verschiedene Verfahren angewandt werden.

Aus dem Stand der Technik ist beispielsweise bekannt, aus Daten einen sogenannten Streuwert (auch als Hash oder Hashwert oder auch Prüfsumme bezeichnet) zu berechnen. Regelmäßig kommt dabei eine sogenannte Streuwertfunktion (Hashfunktion) zum Einsatz. Eine solche Hashfunktion wird beispielsweise durch den sicheren Hash Algorithmus (SHA, secure hash algorithm) bereitgestellt. Mit einer Hashfunktion kann häufig ein in seiner Größe nicht notwendigerweise beschränkter Datenblock auf einen Datenblock fester Größe, den Hash oder Hashwert, abgebildet werden. Eine typische Länge für einen Hash ist beispielsweise 256 bit. Eine wünschenswerte Eigenschaft einer guten kryptologischen Hashfunktion ist eine näherungsweise Injektivität und eine dadurch erzielte näherungsweise Kollisionsresistenz. Die „ideale Hashfunktion" ist daher vollständig linkseindeutig und kollisionsfrei und bildet unterschiedliche Eingangsdaten immer auf unterschiedliche Hashes ab. Das Transmission Control Protocol (TCP) ist ein typischer Anwendungsfall für eine Hashfunktion, wobei ein Hashwert für eine größere Datenmenge berechnet wird. Beispielsweise soll eine größere Datenmenge über ein möglicherweise nicht sicheres Übertragungsmedium, wie das Internet, übertragen werden. Zum Beispiel kann durch einen technischen Fehler ein Teil der Daten falsch übertragen werden oder ein Dritter (Angreifer) manipuliert diese Daten. Wenn der Sender der Daten ihren Hashwert berechnet und diesen Hashwert dem Empfänger zur Verfügung stellt, kann der Empfänger die Echtheit und Unverfälschtheit der Daten verifizieren, vorausgesetzt der Hashwert selbst ist echt und verlässlich.

Neben der Überprüfung der Integrität nach einer Übertragung mittels Prüfsummen gibt es noch die Absicherung der Integrität durch Nutzung von Zertifikaten. Diese basiert in der Regel auf der Nutzung asymmetrischer Verschlüsselung, bei der ein Webservice ein Zertifikat bereitstellt, in dem eine vertrauenswürdige Instanz (Certificate Authority) für die Identität des Webservices garantiert (durch Signatur mittels eines Zertifikates). Ein Zertifikat enthält dann meist einen öffentlichen Schlüssel, der zur Verschlüsselung der initialen Kommunikation mit dem Webservice genutzt werden kann.

Das Hash-Verfahren bringt jedoch den Nachteil mit sich, dass das Verfahren völlig außer Kraft gesetzt wird, wenn der Hashwert selbst während einer Man-In-The-Middle-Attacke manipuliert wird. In einem Beispiel überträgt ein Benutzer A (z. B. Alice) an einen Benutzer B (z. B. Bob) eine Datei und außerdem den Hashwert der Datei. Ein Angreifer E (z. B. Eve) fängt diese Kommunikation ab und ersetzt die Datei durch eine gefälschte Datei. Die gefälschte Datei enthält gefälschte Daten. Außerdem ersetzt E den Hashwert der Datei durch den Hashwert der gefälschten Datei. Wenn B nun die Daten empfängt und überprüft, indem er die Hashfunktion der Datei selbst berechnet und mit dem Hashwert vergleicht,

kommt er zu dem Schluss, dass die Daten nicht manipuliert wurden. So hat E erfolgreich die Daten manipuliert, ohne dass dies von B festgestellt wurde. Dies kann auch durch gängige Verschlüsselungsmethoden wie SSL nicht notwendigerweise festgestellt werden, da auch die zur Verschlüsselung genutzten Zertifikate durch E ersetzt werden können, sodass beide Parteien verschlüsselt mit E kommunizieren und vermuten, die Verbindung sei sicher.

Man-In-The-Middle Attacken lassen sich weitestgehend vermeiden, indem bei der Kommunikation zwischen A und B beide zuvor austauschen, welche Zertifikate sie voneinander erwarten und dadurch ausschließen können, dass ein Angreifer E die Kommunikation manipuliert. Dieser Vorgang wird als Certificate Pinning bezeichnet.

Um bei der Übertragung Privatsphäre zu gewährleisten, können Nachrichten außerdem kryptographisch verschlüsselt werden. Hierbei werden symmetrische und asymmetrische Verschlüsselung unterschieden.

Bei der symmetrischen Verschlüsselung werden Nachrichten mit einem kryptografischen Schlüssel verschlüsselt, sodass die originale Nachricht durch Dritte nicht eingesehen werden kann. Sie kann nur unter Nutzung des, in der Regel, gleichen Schlüssels entschlüsselt werden. Vorteilhaft an der symmetrischen Verschlüsselung ist die Tatsache, dass das Verfahren relativ simpel, effizient und schnell ist. Nachteilig an der symmetrischen Verschlüsselung ist, dass diese voraussetzt, dass beide bzw. alle vertrauenswürdigen Parteien von Beginn des Nachrichtenaustausch an den Schlüssel kennen, da sowohl das Senden als auch das Empfangen von verschlüsselten Nachrichten die Kenntnis voraussetzt. Gleichzeitig muss gesichert sein, dass auch ausschließlich diese Parteien Kenntnis über den Schlüssel haben. Es ergibt sich dadurch das Problem des sogenannten Schlüsseltauschs über einen potenziell unsicheren digitalen Kommunikationskanal zur Initialisierung einer verschlüsselten Konversation mehrerer Parteien, wenn ein Schlüssel nicht geheim per Bote, manueller Übergabe oder ähnlichen Verfahren übergeben werden kann.

Zu diesem Zweck können beispielsweise asymmetrische Schlüsseltauschverfahren wie der Diffie-Hellman-Schlüsselaustausch eingesetzt werden, bei dem Schlüssel über einen unsicheren, potenziell abgehörten Kanal zwischen zwei Parteien ausgetauscht werden können.

Eine weitere simple Möglichkeit zum Schlüsselaustausch ist eine klassische, sogenannte asymmetrische Verschlüsselung des gemeinsamen Schlüssels durch die Partei, welche eine verschlüsselte Kommunikation initialisiert. Eine solche asymmetrische Verschlüsselung setzt

ein Schlüsselpaar je Kommunikationspartei voraus, einen geheimen bzw. privaten und einen öffentlichen Schlüssel. Der geheime Schlüssel ist nur durch die jeweilige Kommunikationspartei bekannt, sollte nicht geteilt werden, und wird sicher abgespeichert. Der öffentliche Schlüssel ist durch potenzielle Kommunikationspartner bekannt. Nachrichten an eine Partei können mithilfe deren öffentlichen Schlüssels unter Nutzung kryptografischer Algorithmen verschlüsselt werden. Die resultierende Nachricht kann nur vom zugehörigen geheimen Schlüssel entschlüsselt werden, also nur von der zugehörigen Partei. Unter der Voraussetzung, dass die jeweiligen Parteien ihr asymmetrisches Schlüsselpaar generieren und den öffentlichen Schlüssel bereitstellen können, kann ein geheimer Schlüsseltausch mithilfe einer solchen Methode über ein unsicheres Netzwerk stattfinden. Mithilfe einer solchen hybriden Kombination aus symmetrischer und asymmetrischer Verschlüsselung kann die Effizienz der symmetrischen Verschlüsselung genutzt werden, ohne dass der Schlüsseltausch durch Angreifer kompromittiert werden kann.

Asymmetrische Verschlüsselungsarchitekturen, bei der jede Partei einen geheimen Schlüssel besitzt und einen zugehörigen öffentlichen Schlüssel bereitstellt, können nicht nur zum Schlüsselaustausch genutzt werden, sondern im Allgemeinen zur Verschlüsselung beliebiger Daten, zur Authentifizierung sowie zum Signieren von Daten zur Sicherstellung des Manipulationsschutzes.

Die Algorithmen bzw. Funktionen zur Erstellung von kryptografischen Schlüsseln aus beispielweise einer Zufallszahlenreihe müssen spezielle Anforderungen aufweisen. So muss nicht nur der geheime Schlüssel in der Lage sein, die mittels des öffentlichen Schlüssels verschlüsselte Nachricht zu entschlüsseln. Es darf außerdem nicht oder quasi nicht möglich sein, aus dem öffentlichen Schlüssel auf den geheimen Schlüssel zurückzuschließen. Um diese Voraussetzungen zu erfüllen, existieren verschiedene kryptografische Systeme mit verschiedenen Einwegfunktionen, z.B. SHA-2.

Mathematisch ist es nicht bewiesen, dass diese Einwegfunktionen bei asymmetrischen Verschlüsselungsverfahren nicht durch einen Angreifer mit entsprechend hoher Rechenleistung umkehrbar sind, man einen privaten Schlüssel also aus dem öffentlichen Schlüssel ableiten kann. Theoretisch bietet daher eine symmetrische Verschlüsselung wie beispielsweise das One-Time-Pad eine noch höhere Sicherheit als eine asymmetrische Verschlüsselung.

Neben der Manipulationssicherheit und Absicherung der Privatsphäre von Nachrichten, bei der Übertragung zwischen den Kommunikationsparteien im Netzwerk mithilfe beschriebener

Methoden, muss auch die IT-Sicherheit der Nachrichtendaten auf den Endgeräten bzw. Ausgabeeinheiten der Kommunikationsparteien sichergestellt werden. Die beste Verschlüsselung einer Nachricht ist nutzlos, wenn nach dem Entschlüsseln auf dem Endgerät die entschlüsselte Nachricht durch Schadsoftware an Dritte weitergeleitet, anders verschlüsselt oder auf andere Weise kompromittiert wird. Wenn die Netzwerkkommunikation ausreichend geschützt ist, wird ein Angriff auf Knotenpunkte wie Server oder die Endgeräte aus Sicht des Angreifers attraktiver. Es ist somit unerlässlich, die einzelnen Endgeräte der Kommunikationsparteien ebenfalls abzusichern.

Allgemein lässt sich sagen, dass bei der Absicherung von Computergeräten ein Ansatz mit möglichst vielen Schutzmaßnahmen sinnvoll ist, da nahezu jedes Schutzsystem überwunden werden kann, aber insbesondere wirtschaftlich motivierte Angreifer in der Regel zunächst die einfachsten Ziele attackieren, da auch sie einer Gewinnmaximierungsabsicht unterliegen. Viele einfach durchzuführende Angriffe sind in der Regel profitabler als der Angriff auf ein komplex abgesichertes System. Daher überwiegt der Nutzen weiterer Schutzschichten im Regelfall überproportional die für zusätzliche Schutzschichten aufgewendeten Kosten.

Die erste Schutzmaßahme, die einem Angreifer entgegensteht, ist meist eine Firewall, die sowohl ein- als auch ausgehende Kommunikation überwacht und eine Zuordnung von Prozessen auf dem Computer zu bestimmten Protokollen, Ports, URLs sowie IP-Adressen erlaubt. Dabei kann ein Blacklisting, also eine negative Bestimmung bzw. Verbot von Zugriffsrechten oder ein Whitelisting, eine positive Bestimmung bzw. Erlaubnis von Zugriffsrechten erfolgen.

Antivirenprogramme überprüfen zusätzlich regelmäßig die permanenten Speicher eines Computers auf bekannte Schadprogramme. Dafür sammelt der Anbieter eines Antivirenprogramms Signaturen bekannter Schadsoftware und häufig auch bestimmte Verhaltensmuster. Nachteilig dabei ist, dass das Überprüfen des Speichermediums auf diese Weise zum einen relativ rechen- und somit zeitaufwändig ist. Zudem ist erforderlich, dass Schadsoftware bereits zumindest teilweise bekannt ist. Neben der Lösung mittels Antivirenprogrammen, bei der eine negative Berechtigungsliste (Programme, die nicht erlaubt werden) geführt wird, besteht auch die Möglichkeit zum Whitelisting, wobei nur bestimmte Anwendungen zugelassen werden, deren Integrität wiederum häufig durch Prüfsummen sichergestellt wird.

Eine weitere mögliche Schutzmaßnahme stellt die Isolation verschiedener Dienste in getrennte Computersysteme dar. Anstatt mehrere Services auf einem Computer innerhalb

eines Betriebssystems bereitzustellen, werden diese Services bspw. auf unterschiedliche virtuelle Maschinen oder Container verteilt, wodurch nicht jede Kompromittierung eines der verteilten Systeme zur Kompromittierung aller Systeme führt.

Als weitere Schutzmaßnahme zur Sicherung von IT-Systemen dient das Berechtigungsmanagement, das die sinnvolle Verwaltung von Zugangsberechtigungen regelt. Nach dem „Principle of least privilege" sollten Anwendungen und Prozesse nur mit den minimal nötigen Berechtigungen gestartet werden.

Zero-Trust nennt sich ein Prinzip in der IT-Sicherheit, bei dem Berechtigungen für den Zugriff auf jegliche Ressourcen nach dem Prinzip „vertraue niemandem" erfolgt. Kein Nutzer erhält Zugriff durch Vertrauensvorschuss, sondern jeder Nutzer muss sich authentifizieren bzw. jeder Zugriff muss verifiziert werden.

Ferner sollten Strukturen im Dateisystem nur insofern veränderbar sein, wie dies für den jeweiligen technischen Nutzer notwendig ist. Dieser könnte bspw. Leseberechtigung für die entsprechende Konfiguration haben, ohne die Konfiguration auch schreiben zu können.

In der Praxis ist diese Maßnahme sehr aufwendig und es kommt immer wieder zu Fehlkonfigurationen, da die korrekte Konfiguration des Berechtigungsmanagements sehr komplex und unübersichtlich ist. Für viele Computeranwendungen des Alltags und deren Betriebssysteme ist ein umfangreiches Berechtigungsmanagement durch die vielfältige Nutzung wenig praktikabel.

Heutige mobile Endgeräte sind für die Verarbeitung und Kommunikation hochsensibler Daten aus Sicht der IT-Sicherheit anspruchsvoll. Die Geräte sind hochkonnektiv, in der Regel dauerhaft mit dem Internet verbunden und viele Anwendungen besitzen Berechtigungen zur Kommunikation. Ein restriktives Berechtigungsmanagement ist durch die Limitierungen bei der Benutzerfreundlichkeit sowie die häufig teilweise private Nutzung der Geräte nur begrenzt umsetzbar. Durch die steigende Funktionalität mobiler Endgeräte steigt deren Komplexität softwareseitig stetig an. Die Bedrohungen der IT-Sicherheit, die ohnehin vielfältiger werden, sind dadurch außerdem schwerer kontrollierbar.

Ein besonders imposantes Beispiel für mächtige Bedrohungen für die IT-Sicherheit mobiler Endgeräte ist die Spyware Pegasus des israelischen Unternehmen NSO, welche seit einigen Jahren für internationale Schlagzeilen sorgt. Die Pegasus Spyware macht sich verschiedene Einfallstore von Mobiltelefonen im Speziellen zum Nutzen. So können Links, die mit dem

Gerät geöffnet werden, für eine Infizierung des Geräts sorgen. Darüber hinaus können aber auch sogenannte Null-Klick-Angriffe durch Ausnutzung von Sicherheitslücken in Kommunikationsanwendungen dafür sorgen, dass ein Nutzer des Mobiltelefons den Angriff kaum verhindern oder naheliegenderweise erkennen kann. Nach der Infizierung des Mobiltelefons ist die Pegasus Software in der Lage Funktionen wie Kamera-, Mikrofon und Dateizugriff erhalten, kann die gewonnenen Daten verpacken und weiterleiten. Dabei kann die Funktion im Entwicklermodus operieren und so umfangreichere Nutzerberechtigungen erhalten als der Nutzer des Mobiltelefons selbst.

Die Vielfältigkeit und potenzielle Unerschöpflichkeit der Einfallstore für solche Schadsoftware und die hohen potenziellen Schäden, die durch die umfangreichen Berechtigungen der Software entstehen, rückten die fehlende IT-Sicherheit von Endgeräten besonders in den Fokus. Pegasus wurde in mindestens 45 Staaten weltweit erfolgreich zum Ausspähen von Regierungsmitgliedern oder -kritikern, Journalisten und Aktivisten, unter anderem durch Geheimdienste vielerlei Länder, eingesetzt.

Die Möglichkeit einer solch umfangreichen feindlichen Infektion eines hochkomplexen Systems mit vielerlei potenziellen Schwachstellen - im Beispiel von Pegasus eines Mobiltelefons - bedeutet, dass grundsätzlich für jede entschlüsselte und digital vorliegende Information von einer Kompromittierung der Integrität und Privatsphäre dieser Information ausgegangen werden muss. Jeder Vorgang auf einem potenziell infizierten Endgerät nach dem Entschlüsseln, beispielsweise das Lesen und Antworten auf den Klartext innerhalb einer Messenger-App, ist dann ein unsicherer Vorgang.

Digitale Kommunikationsschnittstellen bieten das Potenzial zur Manipulation oder Verletzung der Privatsphäre eines Endgerätes. Um dies zu erreichen, können Angreifer Schwachstellen einer Kommunikationsanwendung missbrauchen, indem sie den sogenannten Interpreter des Softwarecodes mit speziell konstruierten Eingaben zum Beispiel Befehle ausführen lassen, die nicht intendiert oder zu denen der Angreifer nicht berechtigt ist. Ein prominentes Beispiel für solche Code Injektion ist ein Angriff auf SQL-Datenbanken mittels SQL-Injektion. Neben einer umsichtigen Programmierung der Kommunikationsanwendung unter Beachtung des jeweiligen Kommunikationsprotokolls können als weitere Maßnahme die verfügbaren Abfrage- und Kommunikationsfunktionen für bestimmte Nutzer möglichst begrenzt werden sowie die Kommunikationskanäle selbst eingeschränkt werden.

Nachfolgend wird die für die Erfindung relevanten Endgeräte der Begriff Ausgabeelemente synonym verwendet, da für die Nachrichtenkommunikation die sichere Nachrichtenausgabe im Zentrum der Erfindung steht. Der Begriff ist dennoch nicht einschränkend auf die Ausgabe

von Nachrichten zu verstehen, andere von der Erfindung umfasste Funktionalitäten werden nachfolgend beschrieben.

AUFGABE

In Anbetracht der beschriebenen Gefährdungssituation durch Bedrohungen von vernetzten, mobilen Endgeräten durch Schadsoftware ist eine völlige oder zumindest annähernde IT-Sicherheit von sensiblen Nachrichten gegen Manipulation und Verletzung der Privatsphäre kaum erreichbar. Es ist daher Aufgabe der vorliegenden Erfindung, eine Vorrichtung und ein Verfahren unter Nutzung von Computerprogrammprodukten bereitzustellen, die eine effektive Schutzschicht für die Kommunikation besonders sensibler Nachrichten zwischen digitalen Endgeräten darstellt. Diese Schutzschicht kann nicht durch eine der im Stand der Technik beschriebenen, softwarebasierten und häufig kompromittierbaren Schutzmaßnahmen umgesetzt werden.

LÖSUNG

Stattdessen soll eine verbesserte Informationssicherheit erreicht werden durch eine physische Trennung der Vorrichtung, die der Entschlüsselung von sensiblen Nachrichten und deren digitaler Ausgabe dient, von dem vernetzten und möglicherweise infizierten Endgerät, das die Nachricht empfängt.

Die Aufgabe wird durch ein computerimplementiertes Verfahren zum Ausgeben und Kommunizieren mit den folgenden Schritten gelöst:

- Identifizieren (S01) einer verschlüsselten ersten Nachricht (1.1) auf einer primären Ausgabeeinheit (2.1),
  wobei die verschlüsselte erste Nachricht (1.1) mit einer spezifischen Verschlüsselungsart (1.3) verschlüsselt worden ist, und
  wobei die verschlüsselte erste Nachricht (1.1) nur mithilfe einer sekundären Ausgabeeinheit (2.2) entschlüsselt werden kann,
- unidirektionales Übertragen (S02) der verschlüsselten ersten Nachricht (1.1) von der primären Ausgabeeinheit (2.1) auf die sekundäre Ausgabeeinheit (2.2), wobei das unidirektionales Übertragen (S02) mittels elektromagnetischer Wellen, vorzugsweise optoelektronisch, mittels Schallwellen und/oder mittels Vibrationen erfolgt, wobei die sekundäre Ausgabeeinheit (2.2) vorzugsweise für das unidirektionale Empfangen von Informationen, insbesondere Daten (2.6)

von der primären Ausgabeeinheit (2.1) eingerichtet ist, vorzugsweise mittels zumindest eines Senders, der zum kabellosen Übertragen bzw. Aussenden von Informationen, insbesondere von Daten (2.6), eingerichtet ist,

wobei das Übertragen vorzugsweise das Empfangen (S02a) der übertragenen ersten verschlüsselten Nachricht (1.1) von der sekundären Ausgabeeinheit (2.2) vorsieht, insbesondere mittels zumindest eines von der sekundären Ausgabeeinheit (2.2) umfassten Empfängers, wobei der Empfänger insbesondere für eine kabellose Datenübertragungstechnologie (2.6), insbesondere zum Empfangen elektromagnetischer Wellen, Schallwellen und/oder Vibrationen, eingerichtet ist,

- Entschlüsseln (S03) der empfangenen ersten verschlüsselten Nachricht (1.1) auf der sekundären Ausgabeeinheit (2.2), wobei das Entschlüsseln mittels zumindest einem von der sekundären Ausgabeeinheit (2.2) umfassten geheimen kryptografischen Schlüssels (1.4) erfolgt,
- Ausgeben (S04) der resultierenden entschlüsselten ersten Nachricht (1.2) auf der sekundären Ausgabeeinheit (2.2), wobei das Ausgeben (S04) insbesondere durch Anzeigen auf einem zur sekundären Ausgabeeinheit (2.2) zugehörigen Ausgabemittel (2.4) erfolgt,
- Eingeben und Verschlüsseln (S05) einer unverschlüsselten zweiten Nachricht auf der sekundären Ausgabeeinheit (2.2), wobei das Eingeben insbesondere mittels eines zur sekundären Ausgabeeinheit (2.2) zugehörigen Eingabemittels (2.5) durchgeführt wird, und wobei das Verschlüsseln der unverschlüsselten zweiten Nachricht, insbesondere mittels kryptografischer Verfahren, eine verschlüsselte zweite Nachricht erzeugt,
- unidirektionales Übertragen (S06) der verschlüsselten zweiten Nachricht von der sekundären Ausgabeeinheit (2.2) auf die primäre Ausgabeeinheit (2.1) mittels einer zur sekundären Ausgabeeinheit (2.2) zugehörigen unidirektionalen Ausgangsverbindung (2.7/2.8), wobei das unidirektionales Übertragen (S06) vorzugsweise als ein elektrisches Signal erfolgt,
- Ausgeben und Kennzeichnen (S07) der verschlüsselten zweiten Nachricht auf der primären Ausgabeeinheit (2.1).

Die Aufgabe wird weiterhin durch ein System zur Datenverarbeitung gelöst, welches das hierin definierte computerimplementierte Verfahren umsetzt. Das System umfasst dabei die sekundären Ausgabeeinheit aus den Verfahrensschritten S01 bis S07 sowie zwei

Computerprogrammprodukte, die die Verfahrensschritte auf der sekundären Ausgabeeinheit sowie der primären Ausgabeeinheit umsetzen.

Weitere vorteilhafte Ausgestaltungen und Weiterbildungen ergeben sich aus den Unteransprüchen sowie aus der Beschreibung unter Bezugnahme auf die Figuren und Ausführungsbeispiele.

ALLGEMEINE VORTEILE

Durch das hierin beschriebene Verfahren kann mit der sekundären Ausgabeeinheit (hierin auch als „sekundäre Ausgabeeinheit" bezeichnet) ein zusätzlicher, sicherer Endpunkt der Kommunikation erzeugt werden. Das bedeutet, dass die primäre Ausgabeeinheit, bspw. ein mobiles Telekommunikationsgerät, wie ein Smartphone, Tablet, Notebook, als Endpunkt, auf welchem eine sensible Nachricht entschlüsselt und angezeigt werden könnte, ersetzt wird. Im Weiteren wird die primäre Ausgabeeinheit hierin auch synonym als ein Endgerät bezeichnet. Durch dieses Verfahren muss ein Nutzer nicht auf die IT-Sicherheit einer, wie der Stand der Technik zeigt, potenziell umfänglich infizierten primären Ausgabeeinheit vertrauen. Stattdessen wird die IT-Sicherheit komplett auf die sekundäre Ausgabeeinheit ausgelagert, sodass die IT-Sicherheit der primären Ausgabeeinheit aus Sicht der Erfindung zu vernachlässigen ist. Gleichzeitig erfüllt die sekundäre Ausgabeeinheit im Wesentlichen nur die Funktionen der Ausgabe von Nachrichten sowie deren Ver- und Entschlüsselung, sodass die Anzahl der Angriffsvektoren, die sich über den Missbrauch von Softwarefunktionen ergeben, äußerst begrenzt ist.

Um einen Zugriff von anderen Komponenten, insbesondere von der primären Ausgabeeinheit, auf die sekundäre Ausgabeeinheit zu vermeiden, und um diese gegenüber Angriffen von Außen abzuschirmen, ist die Datenverbindung von der sekundären Ausgabeeinheit zu der primären Ausgabeeinheit bevorzugt unidirektional ausgebildet. Die eingehende Kommunikation in die sekundäre Ausgabeeinheit ist darüber hinaus grundsätzlich aufgrund der unidirektionalen Ausgangsverbindung auf eine Übertragung mittels der kabellosen Datenübertragungstechnologie, insbesondere durch optoelektronische, akustische und/oder mittels Vibrationen erfolgende Datenübertragung beschränkt, sodass ein potenzieller Angreifer ausschließlich diese Verbindung nutzen und seinen Angriff über diese Datenübertragungstechnologie bereitstellen muss, was eine genereile Hürde darstellt. Über diese Verbindung werden nur in bestimmter Weise verschlüsselte Nachrichten erwartet, die zusätzlich signiert werden können, sodass auch hier die möglichen Angriffsvektoren im Vergleich zu einer vielseitig genutzten Verbindung eines

typischen Endgeräts stark eingeschränkt sind. Durch die Unidirektionalität von Eingang und Ausgang der sekundären Ausgabeeinheit ist es für einen Angreifer unmöglich, direkt durch manipulierte Eingaben Informationen abzufragen.

Vorzugsweise umfasst die verschlüsselte erste Nachricht, die unidirektional von der primären Ausgabeeinheit auf die sekundäre Ausgabeeinheit übertragen wird, eine Signalsequenz, die im Schritt des unidirektionalen Übertragens (S02), insbesondere zu Beginn des unidirektionalen Übertragens (S02), d.h. mit Beginn des Sendens der verschlüsselten ersten Nachricht durch die primäre Ausgabeeinheit die sekundäre Ausgabeeinheit dazu veranlasst, mit dem Aufzeichnen der übertragenen, verschlüsselten ersten Nachricht, zu beginnen.

Vorteilhaft wird durch die Kombination dieser Hürden gegen einen potenziellen Angreifer ein besonders hohes Maß an Datensicherheit und -integrität erreicht, welches für sensible Nachrichten den Mehraufwand eines zusätzlichen Gerätes rechtfertigt.

Außerdem vorteilhaft können die verschlüsselten Nachrichten weiterhin mithilfe der bestehenden primären Ausgabeeinheit empfangen und versendet werden, nur der tatsächliche Endpunkt, an dem die entschlüsselte Nachricht vorliegt und angezeigt wird, wird separiert.

AUSFÜHRLICHE BESCHREIBUNG

Die Erfindung betrifft ein Verfahren zum Ausgeben und Kommunizieren mit den Schritten (S01) bis (S07). Der Schritt des Identifizierens (S01) beschreibt das Kennzeichnen einer eingegangenen verschlüsselten ersten Nachricht auf einem Endgerät, der primären Ausgabeeinheit. Das Identifizieren umfasst hierbei ein Kennzeichnen, das heißt ein visuelles erkenntlich machen für einen Nutzer, sodass dieser erkennen kann, dass die verschlüsselte erste Nachricht eine besonders sensible Nachricht ist, die vom Verfasser intendiert wurde, nur von einer sekundären Ausgabeeinheit bzw. sekundären Ausgabeeinheit entschlüsselt und angezeigt zu werden. Das Identifizieren kann aufgrund einer einzigartigen Zeichenkombination oder eines eindeutigen Zeichenmusters in der verschlüsselten ersten Nachricht geschehen, bevorzugt aber auf Basis einer für diese Nachrichtenart spezifischen digitalen Signatur. In dieser bevorzugten Ausgestaltung kann ein später beschriebenes Computerprogrammprodukt mithilfe eines für die Applikation spezifischen Schlüssels die erste Nachricht überprüfen und dadurch feststellen und kennzeichnen, dass eine sekundäre Ausgabeeinheit zur Entschlüsselung benötigt wird. Vorteilhaft kann mithilfe einer digitalen

Signatur auch die Integrität der verschlüsselten ersten Nachricht geprüft werden, das heißt, dass diese mit der versendeten Version übereinstimmt. Wie später beschrieben wird dieser Schritt allerdings bevorzugt auf der sekundären Ausgabeeinheit durchgeführt.

Im Schritt des unidirektionalen Übertragens (S02) wird die verschlüsselte erste Nachricht vorzugsweise kabellos unidirektional an die sekundäre Ausgabeeinheit übertragen. Bei diesem Verfahren wird vorzugsweise ein auf der primären Ausgabeeinheit vorhandener Sender für eine kabellose Datenübertragungstechnologie verwendet. Die kabellose Datenübertragungstechnologie ist insofern von der Ausstattung der primären Ausgabeeinheit abhängig. Eine genauere Beschreibung der möglichen Datenübertragungstechnologien findet sich weiter unten.

Für das unidirektionale Übertragen (S01) der verschlüsselten ersten Nachricht, weist die primäre Ausgabeeinheit vorzugsweise ein Ausgabeelement auf, der das (Aus-)Senden einer Nachricht durch optoelektronische, akustische und/oder mittels Vibrationen erfolgende Datenübertragung erlaubt.

Um die Nachricht im Schritt des unidirektionalen Übertragens (S02) auf der sekundären Ausgabeeinheit zu empfangen, muss diese zumindest einen Empfänger für die verwendete Datenübertragungstechnologie ausweisen.

Grundsätzlich bietet die kabellose Datenübertragung die einzige Möglichkeit für einen potenziellen Angreifer, Daten an die sekundäre Ausgabeeinheit zu senden, um diese unbemerkt zu manipulieren, während sich die sekundäre Ausgabeeinheit nicht im Besitz des Angreifers befindet. In einer bevorzugten Ausgestaltung des Verfahrens wird vom Nutzer, sobald eine Nachricht an die sekundäre Ausgabeeinheit übertragen werden soll, der Sender für die vom Nutzer ausgewählte Datenübertragungstechnologie erst aktiviert, sodass für einen potenziellen Angriff ein geringes Zeitfenster, eine eingeschränkte Datenübertragungstechnologie und potenziell ein Zufallsfaktor, welche Datenübertragungstechnologie der Nutzer verwenden wird, im Weg stehen. Die verwendeten Datenübertragungstechnologien werden bevorzugt so ausgewählt, dass ein Angreifer nicht über weite Distanzen Nachrichten manipulieren oder einschleusen kann, also auf kurze Distanzen optimiert sind. In einer besonders bevorzugten Ausgestaltung der Erfindung sind die Datenart, die eine sekundäre Ausgabeeinheit im Schritt des unidirektionalen Übertragens (S02), insbesondere beim Empfangen (S02a) erwartet und die entsprechenden Funktionen, die daraufhin ausgeführt werden können, besonders stark eingeschränkt, sodass potenzielle Angriffsvektoren durch manipulierte übertragene Daten weiter begrenzt

werden. In einer bevorzugten Ausgestaltung haben übertragene, insbesondere positiv empfangene, Daten keinerlei Zugriff auf das Speichermedium der sekundären Ausgabeeinheit und werden ausschließlich in einer temporären Speichervorrichtung zwischengespeichert. In dieser Ausgestaltung begrenzen sich die Funktionen zur Datenverarbeitung eingehender Nachrichten innerhalb der sekundären Ausgabeeinheit auf die reine Ausgabe von Daten als graphische und/oder akustische Elemente, wie Bilder, Textbausteine oder Töne, insbesondere auf die reine Ausgabe von Textbausteinen.

Die unidirektionale, insbesondere die kabellose, Datenübertragung bewirkt vorteilhaft im Vergleich zu einer kabelgebundenen Datenübertragung eine weitere Technologiehürde für einen Angreifer, der einen Sender, ein spezifisches von der sekundären Ausgabeeinheit erwartetes Sendesystem oder Sendeprotokoll sowie eine korrekte Ausrichtung von Sender und Empfänger bereitstellen muss. Für den Nutzer hingegen ist die unidirektionale, insbesondere die kabellose, Datenübertragung kaum ein Mehraufwand und kann die Menge der möglichen nutzbaren primäres Ausgabeeinheiten erweitern.

Nach einer bevorzugten Ausgestaltung der Erfindung werden die primäre Ausgabeeinheit und die sekundäre Ausgabeeinheit zum unidirektionalen Übertragen von Daten in unmittelbare Nähe zueinander gebracht. Insbesondere für den Fall, dass das unidirektionale Übertragen optoelektronisch und/oder mittels Vibrationen erfolgt, werden die beiden Ausgabeeinheit vorzugsweise in Kontakt zueinander gebracht. Ein einfaches Beispiel für ein optoelektronisch zu erfolgendes Übertragen der verschlüsselten ersten Nachricht auf die sekundäre Ausgabeeinheit kann vorsehen, dass ein optoelektronisches Ausgabeelement (Sender), bspw. ein Display oder eine einzelne Diode, der primären Ausgabeeinheit derart zu einem optoelektronischen Detektor (Empfänger) der sekundären Ausgabeeinheit angeordnet ist, dass der optoelektronischen Detektor das Signal des optoelektronischen Ausgabeelement erfassen kann. Bspw. ist der optoelektronische Detektor in Deckung mit dem optoelektronischen Ausgabeelement gebracht. So kann ein entsprechender optoelektronischer Detektor der sekundären Ausgabeeinheit bspw. zumindest einen Teil des Displays der primären Ausgabeeinrichtung überlappend, bevorzugt das Display abdeckend, angeordnet sein.

Zur Erhöhung der Sicherheit kann weiterhin vorgesehen sein, dass die sekundäre Ausgabeeinheit ein Angriffsdetektionselement umfasst, das dazu eingerichtet ist, eine veränderte und/oder manipulierte Signatur einer übertragenen, verschlüsselten ersten Nachricht zu detektieren (Intrusion Detection System). Dies bedeutet auch, dass ein Teil der Intelligenz der sekundären Ausgabeeinheit bereits innerhalb des Übertragens eines

Eingangssignals, insbesondere einer verschlüsselten ersten Nachricht, realisieren kann, ob Teile des Systems, das gesamte System oder eine Nachricht der primären Ausgabeeinheit korrumpiert sind. Beispielsweise können durch das Angriffsdetektionselement nur spezielle Signale erkannt werden, die bspw. bereits vorgefiltert sind und/oder Ergebnis einer Vorauswertung sind. In dem Kontext mit dem Angriffsdetektionselement ist es besonders vorteilhaft, wenn die sekundäre Ausgabeeinheit als System zum Erkennen und Verhindern von Eindringlingen (Intrusion Detection and Prevention System) ausgebildet ist, d.h., wenn zudem eine Schutzmaßnahme, als Reaktion auf ein als zumindest teilweise korrumpiert detektiertes System oder auf eine als zumindest teilweise korrumpiert detektierte Nachricht, in Form von Maßnahmensignalen von der sekundären Ausgabeeinheit über diese unidirektionale Verbindung an eine als korrumpiert identifizierte primäre Ausgabeeinheit, insbesondere an korrumpierte Komponenten der primären Ausgabeeinheit, wie bspw. die Datenverarbeitungseinrichtung und/oder an alle Recheneinheiten der primären Ausgabeeinheit übermittelt werden. Auf diese Weise kann als Schutzmaßnahme das Abschalten und/oder Resetten der primären Ausgabeeinheit, insbesondere von Recheneinheiten und/oder weiteren Komponenten der primären Ausgabeeinheit und/oder die Veränderung von Betriebsparametern, beispielsweise von Zugriffserlaubnissen, umfassen. Auch die Beendigung und der Neustart bestimmter Applikationen (falls das System nur teilweise korrumpiert ist) sind denkbar. Darüber hinaus kann das Übertragen eines Maßnahmensignals von der sekundären Ausgabeeinheit an die primäre Ausgabeeinheit vorgesehen sein, der einen Kurzschluss in der primären Ausgabeeinheit vorsieht, zum Einsatz kommen und hierdurch die primäre Ausgabeeinheit ausschaltet oder deaktiviert.

Zweckmäßigerweise kann bei dem Detektieren einer veränderten und/oder manipulierten Signatur einer übertragenen, verschlüsselten ersten Nachricht oder dem Klassifizieren der primären Ausgabeeinheit als korrumpiert durch das Angriffsdetektionselement der sekundären Ausgabeeinheit ein Melden dieses Zustands an eine externe Recheneinrichtung vorgesehen sein.

Im Schritt des Entschlüsselns (S03) wird die verschlüsselte erste Nachricht entschlüsselt und vorzugsweise auf einem optoelektronischen Ausgabeelement, bspw. einem Display, der sekundären Ausgabeeinheit für den Nutzer ausgegeben bzw. angezeigt. Das optoelektronische Ausgabeelement ist bspw. ein Display, das in einer bevorzugten Ausgestaltung, in der nur Textdaten versendet werden, als ein simples, einfarbiges Display zur effizienten Darstellung einer moderaten Anzahl an Textzeilen ausgeführt sein kann. Verschiedene Ausgestaltungen der Entschlüsselung sind in der Beschreibung der

Unteransprüche beschrieben. Der kryptografische Schlüssel zum Entschlüsseln ist grundsätzlich geheim zu halten und wird vorzugsweise nur auf dem Speichermedium der sekundären Ausgabeeinheit gespeichert. In einer bevorzugten Ausführung haben Nachrichten keinerlei Zugriff oder Auswirkungen auf dieses Speichermedium, sodass der kryptografische Schlüssel nicht durch Nachrichten, insbesondere durch übertragene bzw. empfangene Nachrichten, manipuliert werden kann, aber von Beginn der Auslieferung der sekundären Ausgabeeinheit an einen Nutzer dort vorliegt. Bspw. kann der kryptografische Schlüssel direkt bei der Herstellung der sekundären Ausgabeeinheit auf das Speichermedium, bspw. einen Chip hinterlegt und/oder eingebracht werden. In einer alternativen Ausführung kann der kryptografische Schlüssel durch die Übertragung einer speziellen, in ihrer Verschlüsselung oder Signatur einzigartigen Nachrichtenart auf der sekundären Ausgabeeinheit gespeichert werden. Diese Signatur kann wahlweise nur durch Administratorgeräte, den Hersteller oder für eine einmalige Initialisierung der sekundären Ausgabeeinheit erzeugt werden. Durch diese Ausführungen ist eine gewisse Flexibilität für eine Änderung des kryptografischen Schlüssels bei sehr hoher IT-Sicherheit gegeben.

Der Schritt (S05) umfasst das Eingeben und Verschlüsseln einer Nachricht auf der sekundären Ausgabeeinheit. Das Eingeben geschieht mithilfe eines Eingabemittels, welches in einer möglichen Ausführung als Tastatur mit physischen Knöpfen ausgestaltet ist. Vorteilhaft ist diese Ausführung robust und preisgünstig. Sie kann dann eingesetzt werden, wenn in einer Ausführung gleichzeitig die angezeigten Nachrichten auf Textnachrichten begrenzt sind, da in diesem Fall ein geringeres Maß an Flexibilität des Eingabemittels erforderlich ist. In einer anderen, bevorzugten Ausführung ist das Eingabemittel als Touchscreen oder Touchpad ausgestaltet. Diese Variante erlaubt eine höhere Flexibilität bei der Eingabe von diverseren Zeichen, falls nicht nur simple Textnachrichten verfasst werden sollen. Zudem erlauben es Touchscreens oder Touchpads, dass diese aus einem flexiblen Material gebildet sein können und dadurch an die Geometrie der primären Ausgabeeinheit angepasst werden können. Dies bietet sich insbesondere für den Fall an, dass die sekundäre Ausgabeeinheit zumindest einen Teil des Displays der primären Ausgabeeinrichtung überlappend, bevorzugt das Display abdeckend, angeordnet ist.

Für Ausführungen des Verschlüsselns sei auf die Beschreibung des Schrittes (S05) und auf die späteren Beschreibungen der Unteransprüche verwiesen.

Aus den Schritten (S04) und (S05) ergibt sich, dass die entschlüsselten Nachrichten, die von der sekundären Ausgabeeinheit empfangen bzw. an diese übermittelt oder ausgesendet werden sollen, in entschlüsselter Form ausschließlich auf dieser sekundären Ausgabeeinheit

vorliegen und auf keiner anderen informationstechnischen Einheit, insbesondere keinem anderen Endgerät, entschlüsselt sind, wodurch sich vorteilhaft sowohl Übertragungssicherheit wie auch Endpunktsicherheit für diese Nachrichtenkommunikation ergibt.

In Schritt (S06) wird ein unidirektionales Übertragen der Nachricht zurück an die primäre Ausgabeeinheit umgesetzt. Mögliche Ausführungsvarianten dieser Übertragung beinhalten kabellose Varianten, wobei diese derart ausgestaltet sind, dass die sekundäre Ausgabeeinheit nur den Sender umfasst. Die Übertragung kann allerdings bevorzugt auch kabelgebunden erfolgen. In diesem Kontext ist es besonders vorteilhaft, wenn eine Schutzmaßnahme in Form von Maßnahmensignalen über diese unidirektionale Verbindung an eine als korrumpiert identifizierte primäre Ausgabeeinheit, insbesondere an korrumpierte Komponenten der primären Ausgabeeinheit, wie bspw. die Datenverarbeitungseinrichtung und/oder an alle Recheneinheiten der primären Ausgabeeinheit übermittelt werden. Auf diese Weise kann als Schutzmaßnahme das Abschalten und/oder Resetten der primären Ausgabeeinheit, insbesondere von Recheneinheiten und/oder weiteren Komponenten der primären Ausgabeeinheit und/oder die Veränderung von Betriebsparametern, beispielsweise von Zugriffserlaubnissen, umfassen. Auch die Beendigung und der Neustart bestimmter Applikationen (falls das System nur teilweise korrumpiert ist) sind denkbar. Darüber hinaus kann das Übertragen eines Maßnahmensignals von der sekundären Ausgabeeinheit an die primäre Ausgabeeinheit vorgesehen sein, der einen Kurzschluss in der primären Ausgabeeinheit vorsieht, zum Einsatz kommen und hierdurch die primäre Ausgabeeinheit ausschaltet oder deaktiviert.

In Schritt (S07) wird die von der sekundären Ausgabeeinheit übertragene und von der primären Ausgabeeinheit empfangene Nachricht auf der primären Ausgabeeinheit identifiziert und als sensible, verschlüsselte Nachricht gekennzeichnet, vergleichbar mit dem Schritt des Identifizierens bzw. Kennzeichnens (S01), mit dem Unterschied, dass hier eine ausgehende Nachricht markiert wird.

In einer bevorzugten Ausführung der Schritte (S01) und (S07) des beschriebenen Verfahrens wird das Anzeigen und Kennzeichnen von eingehenden und ausgehenden verschlüsselten Nachrichten, die nur auf einer sekundären Ausgabeeinheit entschlüsselt werden können, mithilfe von sogenannten Add-Ins auf der primären Ausgabeeinheit durchgeführt. Das bedeutet, dass existierende Apps zur Kommunikation von Nachrichten, beispielsweise internetbasierte Messenger Dienste wie Whatsapp, Signal oder Facebook oder Mail Applikationen um Funktionen erweitert werden, die eine beschriebene Kennzeichnung der

speziell verschlüsselten Nachrichten umfassen. Außerdem umfassen diese Anwendungen Funktionen, um den Schritt des Übertragens (S02) zu initialisieren.

In einer alternativen, bevorzugten Ausführung wird außerdem eine Funktion im Betriebssystem der primären Ausgabeeinheit registriert, welche beim Klick auf eine beschriebene sensible Datei die Datenart erkennt und die Option anbietet, diese Datei mittels Initialisierung von Schritt (S02) zu übertragen.

In einer alternativen bevorzugten Ausführung der Schritte S01 und S07 des beschriebenen Verfahrens wird das Identifizieren und Kennzeichnen von eingehenden und ausgehenden verschlüsselten Nachrichten, die nur auf einer sekundären Ausgabeeinheit entschlüsselt werden können, mithilfe einer eigenen Applikation auf der primären Ausgabeeinheit durchgeführt. In einer besonders bevorzugten Ausführung ist diese Applikation eine eigene Kommunikationsapplikation, mit der bevorzugt internetbasiert Nachrichten versendet werden können. In dieser speziellen Ausführung umfasst der Schritt (S01) entsprechend außerdem das Empfangen von Nachrichten in der eigenen Applikation und der Schritt (S07) außerdem das Senden von Nachrichten in der eigenen Applikation.

Besonders bevorzugt kann in dieser Applikation beim Versenden von Nachrichten zwischen drei Sicherheitsstufen gewählt werden: Die niedrigste Sicherheitsstufe sind unverschlüsselte Nachrichten, die zwischen Endgeräten versendet werden. Die mittlere Sicherheitsstufe sind verschlüsselte Nachrichten, die auf den Endgeräten entschlüsselt werden, wobei beachtet werden muss, dass ein Endgerät potenziell infiziert sein kann. Die höchste Sicherheitsstufe wird durch Nachrichten erreicht, die auf einer sekundären Ausgabeeinheit ver- und entschlüsselt werden und von der Applikation entsprechend wie Dateianhänge behandelt werden, die als zusätzlicher Aktion der restlichen Verfahrensschritte (S02) bis (S06) bedürfen. In einer weiterhin bevorzugten Ausführung umfasst die beschriebene eigene Applikation die Registrierung einer Funktion im Betriebssystem, wodurch sensible verschlüsselte Dateien, die über andere Dienste zur Kommunikation von Nachrichten erhalten wurden, mithilfe dieser Applikation geöffnet werden können. Die weiteren Schritte, insbesondere Schritt (S02), können dann aus der Applikation initialisiert werden.

In einer bevorzugten Ausführungsvariante basiert das unidirektionale Übertragen (S02), die in den Schritten (S02) und (S03a) verwendet wird, auf einer kabellosen Datenübertragungstechnologie, insbesondere auf elektromagnetischen Wellen, besonders bevorzugt auf einer optoelektronischen Übertragung. In einer besonders bevorzugten Ausführung wird ein sogenannter Optokoppler verwendet, welcher bevorzugt aus einer LED

als Sender an der primären Ausgabeeinheit und einem Fototransistor als Empfänger an der sekundären Ausgabeeinheit besteht. Mithilfe dieses Aufbaus können digitale und analoge Signale übertragen werden. Die höchstmöglich erreichbare Frequenz von Optokopplern liegt im GHz Bereich, sodass Textnachrichten problemlos schnell übertragen werden können. Für die Ausführung wird bevorzugt ein Verbindungselement zur korrekten Ausrichtung von Sender und Empfänger, sowie bevorzugt ein Gehäuse um Sender und Empfänger verwendet, um fehlerhafte Signale zu vermeiden. Vorteilhaft an dieser Ausgestaltung ist, dass Smartphones, als besonders häufig eingesetzte Endgeräte, in der Regel über zumindest eine simple LED verfügen, die bereits im Gerät verbaut sind uns als Sender in Frage kommt.

In einer besonders bevorzugten Ausführung der Variante des Übertragens (S02) mittels elektromagnetischer Wellen, besonders bevorzugt mittels einer optoelektronischen Übertragung, wird das Display der primären Ausgabeeinheit als Sender eingesetzt. Hierbei bietet es sich an, dass ein entsprechender Detektor, der zum Detektieren elektromagnetischer Wellen eingerichtet ist, insbesondere ein optoelektronischer Detektor an der sekundären Ausgabeeinheit so angeordnet sein, dass dieser bspw. zumindest einen Teil des Displays der primären Ausgabeeinrichtung überlappend, bevorzugt das Display abdeckend, angeordnet ist.

In einer weiterhin besonders bevorzugten Ausführung unter Nutzung elektromagnetischer Wellen werden Funkwellen zum Senden verwendet. Funkwellen verschiedener Standards sind in den meisten Endgeräten ebenfalls verbaut, beispielsweise Bluetooth und UMTS, was vorteilhaft für die Konnektivität der Erfindung in dieser speziellen Ausführung ist. Die vielgenutzten und reichweitenstarken Frequenzbänder bieten allerdings Potenzial für Angreifer, fehlerhafte oder bösartige Daten zu Senden. Diese spezielle Ausgestaltung ist insofern bevorzugt mittels eines geheimen Protokolls, einer zusätzlichen Netzwerkverschlüsselung oder vergleichbaren Sicherheitsmaßnahmen auszuführen. In einer alternativen Ausführung mittels Funkwellen wird eine nicht öffentlich genutzte Funkfrequenz verwendet, die abseits vorhandener Standards oder Regularien angesetzt wird. Auf dieser Frequenz zu manipulieren, erfordert wiederum einen erhöhten Aufwand eines potenziellen Angreifers in einem kleinen Zeitfenster während des Nachrichtenaustauschs gemäß der Erfindung. In einer bevorzugten Ausführung kann diese Funkfrequenz bei jeder Nutzung variiert werden. Nachteilig ist hierfür in der Regel ein zusätzlich Funkmodul zum Senden für die primäre Ausgabeeinheit notwendig.

In einer besonders bevorzugten Ausführung der Variante mittels Funkwellen wird der Near Field Communication (NFC) Standard verwendet, welcher mittels elektromagnetischer Induktion die Nachrichtenübertragung mit mittlerer Bandbreite über geringe Entfernungen erlaubt. Diese Technologie ist bereits in den meisten modernen Smartphones verbaut und ermöglicht insbesondere sensible Anwendungen wie die kontaktlose Kartenzahlung oder Ausweisauthentifizierung. Durch die geringen möglichen Maximalabstände ist eine hohe Manipulationssicherheit natürlicherweise gegeben. Zusätzliche Sicherheitsmaßnahmen, beispielsweise zur Authentifizierung der korrekten beteiligten Geräte, können zusätzlich veranlasst werden.

In einer alternativen Ausführungsvariante basiert die kabellose Datenübertragungstechnologie, die in den Schritten (S02) und (S02a) verwendet wird, auf Schallwellen. Schallwellen können vorteilhaft von den meisten Endgeräten, wie Smartphones oder Notebooks, bereits ausgesendet werden. Schallwellen können in hörbaren, aber bevorzugt auch in nicht hörbaren Frequenzen zur Datenübertragung genutzt werden. Dagegen gestaltet sich eine vollständige Abschirmung zur störungsfreien Übertragung anspruchsvoll, sodass in der Regel auf Seiten der sekundären Ausgabeeinheit Funktionen zum Filtern der Signale zusätzlich implementiert werden müssen und bestimmte Umgebungsvoraussetzungen bei der Übertragung erfüllt werden müssen.

In einer weiteren alternativen Ausführungsvariante basiert die kabellose Datenübertragungstechnologie, die in den Schritten (S02) und (S02a) verwendet wird, auf Vibration. Die Übertragung wird demnach mittels Körperkontakt und mechanischer Schwingung zwischen der primären Ausgabeeinheit und der sekundäre Ausgabeeinheit erreicht. Auch hierfür sind ein korrekter Kontakt und eine störungsfreie Umgebung der Geräte notwendig. Vorteilhaft beinhaltet in der Regel jedes Smartphone einen Vibrationsmotor, gleichzeitig ist aus Sicht eines Angreifers eine solche Übertragungsart untypisch und daher ein schmaler Angriffsvektor.

Grundsätzlich ist für die Schritte (S02) und (S02a) zu beachten, dass für die Nutzung kabelloser Datenübertragungstechnologien in der Regel auf eine physisch korrekte Ausrichtung beider Geräte zueinander zu achten ist, die für die Nachrichtenübertragung vorausgesetzt wird.

Nach einer bevorzugten Ausführung des Verfahrens wird zumindest für den Schritt des Entschlüsselns (S03) einer Nachricht zusätzlich zum kryptografischen Schlüssel ein externer Schlüssel verwendet. In dieser Ausführung müssen beide Schlüssel vorhanden sein, um die

Nachricht entschlüsseln zu können. In einer besonders bevorzugten Ausführung des Verfahrens ist dieser Schlüssel auf einer externen Speicherkarte gespeichert. Eine solche Speicherkarte ist vorteilhaft besonders klein, leicht und günstig, um Schlüssel zu speichern und in alle befugten sekundären Ausgabeeinheit zu integrieren.

Ein solcher zusätzlicher externer Schlüssel kann vorteilhaft die Sicherheitsstufe einer verschlüsselten Nachricht erhöhen. Ein denkbarer Einsatzzweck ist es, dass innerhalb einer Behörde sensible Nachrichten grundsätzlich zwischen sekundären Ausgabeeinheit versendet und von diesen auch entschlüsselt werden können. Mitglieder der Führungsebene können ihre Nachrichten aber mit einem zusätzlichen Schlüssel verschlüsseln, sodass die Empfänger einen entsprechenden externen Schlüssel an ihren sekundären Ausgabeeinheit benötigen. In einem alternativen Einsatzzweck können durch zusätzliche externe Schlüssel hochsensible Nachrichten zwischen Ressorts getrennt werden, beispielsweise zwischen verschiedenen Ministerien oder Abteilungen. Wird eine Nachricht aus Versehen an einen falschen Empfänger mit sekundärer Ausgabeeinheit und korrektem kryptografischem Schlüssel gesendet oder in einer großen Organisation eine Nachricht fehlerhaft versendet, kann diese Maßnahme die Privatsphäre absichern.

In einer bevorzugten Ausgestaltung kann durch den Einsatz eines externen Schlüssels zum Entschlüsseln dieser Schlüssel auch zum Verschlüsseln einer Nachricht verwendet werden. Dies ist entweder möglich, weil der externe Schlüssel ein symmetrischer Schlüssel ist, der sowohl zum Ver- als auch zum Entschlüsseln von Nachrichten eingesetzt werden kann. Alternativ wird auf dem Speichermedium des externen Schlüssels zumindest ein entsprechender öffentlicher Schlüssel eines asymmetrischen Schlüsselpaares eines möglichen Empfängers mitgeliefert, mit welchem dieser Empfänger adressiert werden kann, indem eine Nachricht nur für diesen Empfänger verschlüsselt wird.

In einer bevorzugten Ausführung des Verfahrens werden für den Schritt des Entschlüsselns (S03) oder den Schritt des Verschlüsselns (S05) asymmetrische kryptografische Verfahren eingesetzt. Vorteilhaft muss dafür nur ein einziger geheimer Schlüssel plus etwaige externe Schlüssel gespeichert werden, mit dem eingehende Nachrichten entschlüsselt werden können. Zum Verschlüsseln von Nachrichten muss der öffentliche Schlüssel jedes Empfängers auf der sekundären Ausgabeeinheit gespeichert oder zu dieser übertragen werden. Vorteilhaft hierbei ist, dass diese öffentlichen Schlüssel keine sensiblen Inhalte sind.

In einer besonders bevorzugten Ausführung des Verfahrens werden für den Schritt des Entschlüsselns (S03) oder den Schritt des Verschlüsselns (S05) symmetrische

kryptografische Verfahren eingesetzt. Insbesondere bei der beschriebenen Ausführung, welche externe Schlüssel, insbesondere aus externen Speicherkarten umfasst, sind die externen Schlüssel bevorzugt als symmetrische Schlüssel auszuführen. Symmetrische kryptografische Verfahren haben den Vorteil, dass der gleiche Schlüssel zum Ver- und Entschlüsseln eingesetzt werden kann, solange der Absender und der Empfänger über diesen Schlüssel verfügen. Weiterhin vorteilhaft ist die effizientere und noch sicherere Verschlüsselungstechnologie im Vergleich zu asymmetrischen kryptografischen Verfahren.

Eine Herausforderung für die Ausführung unter Nutzung symmetrischer kryptografischer Verfahren ist der Schlüsseltausch unter den befugten Korrespondenten, aber ausschließlich unter diesen. Ein externer Schlüssel ist hierfür perfekt geeignet, da das Speichermedium, bevorzugt die externe Speicherkarte, immer geheim an den korrekten Empfänger übergeben werden muss, unabhängig ob ein symmetrisches oder asymmetrischen Verschlüsselungssystem durch den externen Schlüssel genutzt wird. Wird allerdings über ein Netzwerk erstmals eine Verbindung mit einer neuen sekundären Ausgabeeinheit aufgebaut, welche Nachrichten senden oder empfangen soll, müssen symmetrische Schlüssel ausgetauscht werden. Hierfür eignen sich wiederum asymmetrische kryptografische Verfahren, sodass in einer besonders bevorzugten Ausführung des Verfahrens sowohl symmetrische als auch asymmetrische kryptografische Verfahren für die Ver- oder Entschlüsselung gemeinsam verwendet werden.

In einer weiteren, bevorzugten Ausführung des Verfahrens umfasst der Schritt des Entschlüsselns (S03) zusätzlich das Prüfen einer digitalen Signatur. Außerdem umfasst in dieser Ausführung das Verfahrensmerkmal Verschlüsseln des Schritts S05 zusätzlich das Hinzufügen einer digitalen Signatur. Mithilfe einer digitalen Signatur kann vorteilhaft sichergestellt werden, dass die Nachricht auf den primären Ausgabeeinheiten oder im unsicheren Netzwerk nicht manipuliert und verändert wurde. Manipulationssicherheit ist, wie im Stand der Technik beschrieben, ein zweiter großer und vorteilhafter Baustein zusätzlich zur Privatsphäre der Nachrichten durch die Verschlüsselung.

Die Erfindung betrifft neben dem erfindungsgemäßen Verfahren auch eine Vorrichtung, konkret die sekundäre Ausgabeeinheit, welche zusätzlich zur typischerweise verwendeten primären Ausgabeeinheit erfindungswesentlich ist.

Die sekundäre Ausgabeeinheit, ist in ihren Außenmaßen so ausgestaltet, dass sowohl komfortabel Nachrichten angezeigt und eingegeben werden können, gleichzeitig aber die sekundäre Ausgabeeinheit mobil und leicht für die Verwendung unterwegs ist. Bezüglich der

Außenmaße bietet sich daher bevorzugt ein Format ähnlich aktueller Smartphones an. Der Fachmann weiß, dass die Außenmaße der sekundären Ausgabeeinheit variiert werden können. An dieser Stelle sei darauf hingewiesen, dass bestimmte hier oder nachfolgend beschriebene Ausführungsformen, insbesondere bezüglich Eingabemittel, Ausgabemittel und Ausrichtung bzw. Verbindung von primärer Ausgabeeinheit und sekundärer Ausgabeeinheit ebenfalls solche Außenmaße vorteilhaft machen, die gleich denen aktueller Smartphones sind, um ein Höchstmaß an Ergonomie sowie Kompatibilität zu dem mutmaßlich häufigsten verwendeten Endgerät, dem Smartphone, herzustellen. Die sekundäre Ausgabeeinheit umfasst neben ihren Kernkomponenten, die nachfolgend beschrieben werden, bevorzugt einen Akkumulator, der es erlaubt, die sekundäre Ausgabeeinheit mobil einzusetzen.

Die sekundäre Ausgabeeinheit umfasst zumindest die Komponenten Ausgabemittel, Eingabemittel, Empfänger für eine kabellose Datenübertragungstechnologie, unidirektionale Ausgangsverbindung, Speichermedium und Rechenmedium.

Ausführungsvarianten der Komponenten Ausgabemittel und Eingabemittel sind bereits weiter oben beschrieben.

In einer möglichen Ausführung ist das Speichermedium als kleiner Solid-State Speicher ausgeführt. Solid-State Speicher weisen vorteilhaft eine geringe Empfindlichkeit gegenüber Stößen auf und sind klein und leicht umsetzbar. In einer bevorzugten Ausführung ist der Speicher als spezieller „embedded secure chip" ausgestaltet, welche spezielle Eigenschaften für die IT-Sicherheit umfassen, insbesondere Schutz vor Hardwarefehlern und -attacken durch „device hardening", eingebaute Limitierung von Brute-Force-Attacken, integrierte Funktionen zur Verschlüsselung und selbstlöschende Speicher bei physischen Angriffen. In einer besonders bevorzugten Ausführung wird ein solcher embedded secure chip mit einem Solid-State-Speicher kombiniert, um von dem höheren Speicher des Solid-State-Speichers zu profitieren, während sensibles Schlüsselmaterial vorteilhaft auf dem embedded secure chip gespeichert werden kann. In einer alternativen, bevorzugten Variante wird anstelle oder zusätzlich zum Solid-State Speicher ein s-RAM Bauelement als flüchtige Speichereinheit verbaut und es werden Softwaretechnologien eingesetzt, um einen gespeicherten geheimen Schlüssel auf diesem flüchtigen Speicher zu speichern und nur bei angelegter Spannung zur Verfügung zu stellen. Vorteilhaft ergibt sich aus dieser Variante ein Hindernis für einen Angreifer, den Speicher auszubauen und geheime Schlüssel auszulesen.

Vor physischen Angriffen ist das Speichermedium bevorzugt in einer Weise geschützt, dass dieses nicht oder kaum zerstörungsfrei aus dem Gerät entnommen werden kann. Dies wird beispielsweise durch gezielte Verklebungen von beispielsweise Kontakten oder Schichten der Chips erreicht, sodass mechanischer Eingriff zur Zerstörung oder Löschung des Speichers führt. Zusätzlich wird bevorzugt das Speichermedium bevorzugt, besonders bevorzugt durch das Gehäuse, mechanisch und elektrotechnisch nach außen isoliert, sodass durch „Side-Channel-Attacks" oder analytische Angriffe von außen keine Manipulationen vorgenommen oder Informationen extrahiert werden können. Weitere IT-Sicherheitsmaßnahmen entsprechend dem sich dauerhaft weiterentwickelnden Stand der Technik können zusätzlich integriert werden.

In einer bevorzugten Ausführung ist das Rechenmedium als integrierter Microchip ausgeführt. Vorteilhaft wird für die Rechenoperationen zum Ver- und Entschlüsseln, das Hinzufügen von Signaturen sowie die Ausgabe und Eingabe von Textnachrichten eine sehr begrenzte Rechenleistung benötigt. In dieser bevorzugten Ausführung wird der Microchip besonders klein und vorteilhaft stromsparend ausgeführt.

In einer Ausführungsvariante der sekundären Ausgabeeinheit ist die unidirektionale Ausgangsverbindung als unidirektionale Kabelverbindung ausgeführt. Eine solche unidirektionale Kabelverbindung erlaubt es durch elektrotechnische Bauelemente, die Kommunikation auf die Richtung von der sekundären Ausgabeeinheit zur primären Ausgabeeinheit zu beschränken. Diese Beschränkung erlaubt es vorteilhaft einer potenziell infizierten primären Ausgabeeinheit nicht, Manipulationen über diese Schnittstelle an der sekundären Ausgabeeinheit vorzunehmen.

In einer Ausführungsvariante der sekundären Ausgabeeinheit umfasst diese zumindest einen solchen Empfänger für kabellose Datenübertragungstechnologien, wie sie in der Beschreibung des Verfahrens ausgeführt worden. In einer bevorzugten Ausführung umfasst die sekundäre Ausgabeeinheit mehrere Empfänger für verschiedene beschriebene kabellose Datenübertragungstechnologien. In einer besonders bevorzugten Ausgestaltung weist die sekundäre Ausgabeeinheit Empfänger für die kabellosen Übertragungstechnologien ausgewählt aus Optokopplung, Vibration, Funkstandards, nicht-standardisierte Funkfrequenzen und Near Field Communication auf.

In einer weiterhin bevorzugten Ausführungsvariante umfasst die sekundäre Ausgabeeinheit zusätzlich zumindest einen, bevorzugt aber eine größere Anzahl an Anschlüssen für Speicherkarten. Mithilfe dieser Anschlüsse kann vorteilhaft die beschriebene Ausführung des

Verfahrens umgesetzt werden, nach welcher zumindest ein auf zumindest einer externen Speicherkarte gespeicherter externer Schlüssel für zumindest das Entschlüsseln von verschlüsselten Nachrichten verwendet wird.

In einer besonders bevorzugten Ausführungsvariante sind diese Anschlüsse für externe Speicherkarten so ausgestaltet, das einmal verbundene externe Speicherkarten nicht zerstörungsfrei entnommen werden können. Dies hat den Vorteil, das geheime externe Schlüssel auf den externen Speicherkarten nicht von Angreifern gelesen werden können, da bei gewaltvoller Entfernung der externen Speicherkarten deren Speicher zerstört wird. Diese Ausführungsvariante kann beispielsweise durch eine physische Arretierung der Speicherplatine einer externen Speicherkarte im Gehäuse der sekundären Ausgabeeinheit ausgeführt werden, wobei die physische Arretierung dafür sorgt, dass die externe Speicherkarte mittels grober Gewalt aus dem Gehäuse entfernt werden müsste, was wiederum eine besonders hohe Wahrscheinlichkeit der Zerstörung der externen Speicherkarte zur Folge hätte. In einer alternativen Umsetzung dieser Ausführungsvariante muss vor oder bei der Entfernung der externen Speicherkarte ein Mechanismus betätigt werden, welcher den Speicher der externen Speicherkarte zurücksetzt, um diese entfernen zu können.

In einer bevorzugten Ausgestaltung der sekundären Ausgabeeinheit umfasst diese als weitere Komponente Verbindungselemente, welche dazu dienen, die sekundäre Ausgabeeinheit mit der primären Ausgabeeinheit physisch aneinander zu binden. Diese Verbindung hat den technischen Effekt, dass beide Geräte physisch wie ein Objekt handhabbar sind und weiterhin die Position beider Geräte relativ zueinander fixiert ist. Vorteilhaft muss dadurch im Fall der Nutzung der sekundären Ausgabeeinheit diese nicht als zusätzliches Gerät eingesetzt werden, sondern kann physisch an die sowieso vorhandene primäre Ausgabeeinheit angebunden werden, um die Handhabbarkeit durch den Nutzer zu erhöhen. Weiterhin vorteilhaft kann die Positionierung des Senders einer kabellosen Datenübertragungstechnologie an der primären Ausgabeeinheit sowie des Empfängers einer kabellosen Datenübertragungstechnologie an der sekundären Ausgabeeinheit in der relativ zueinander und für die Funktionsweise der kabellosen Datenübertragungstechnologie korrekten Position fixiert werden. Eine mögliche Umsetzung dieser Ausführungsvariante kann durch feste Klemmverbindungen an der sekundären Ausgabeeinheit erreicht werden. Diese setzen weitgehend gleiche Arten von sekundären Ausgabeeinheit und vor allem primären Ausgabeeinheiten voraus, um praktikabel zu sein. Diese Umsetzungsvariante könnte vorteilhaft eingesetzt werden, wenn beispielsweise in einer großen Institution viele gleiche Arten an primären Ausgabeeinheiten, beispielsweise als Dienstmobiltelefone,

eingesetzt werden. Als alternative Umsetzungsvarianten sind flexible formschlüssige Bänder, magnetische Verbindungen oder Saugverbindungen denkbar.

Die vorliegende Erfindung betrifft zudem ein Computerprogrammprodukt S, welches auf dem Speichermedium der sekundären Ausgabeeinheit, wie einer sekundären Ausgabeeinheit, gespeichert ist. Bei Ausführung durch das Rechenmedium der sekundären Ausgabeeinheit veranlasst das Computerprogrammprodukt S die Ausführung der Schritte oder Teile der Schritte (S02a) bis (S06) des Verfahrens. Insbesondere ist das Computerprogrammprodukt S für die Umsetzung aller beschriebenen Ausführungsformen des Empfangens der Nachrichten über einen Empfänger für eine kabellose Datenübertragungstechnologie, des Überprüfens des Kommunikationsprotokolls und etwaiger digitaler Signaturen, des Entschlüsselns der Nachrichten, des Anzeigens der Nachrichten auf dem Ausgabemittel, des Eingebens von Nachrichten mittels des Eingabemediums, des Verschlüsselns von Nachrichten und Hinzufügen von Signaturen, des Einbeziehens von externen Schlüsseln in das Ent- und Verschlüsseln von Nachrichten, sowie des unidirektionalen Übertragens von Nachrichten an die primäre Ausgabeeinheit, verantwortlich.

Entsprechend der beschriebenen Ausführungsvarianten des Verfahrens und der sekundären Ausgabeeinheit kann dieses Computerprogrammprodukt S in seinem Funktionsumfang sehr unterschiedlich umfangreich ausgestaltet sein.

Die vorliegende Erfindung betrifft zudem ein Computerprogrammprodukt E, welches auf einem Speichermedium der primären Ausgabeeinheit gespeichert ist. Bei Ausführung durch ein Rechenmedium der primären Ausgabeeinheit veranlasst dieses Computerprogrammprodukt E die Schritte oder Teile der Schritte (S01), (S02) und (S07) des Verfahrens. Insbesondere ist dieses Computerprogrammprodukt S für die Umsetzung aller beschriebenen Ausführungsformen des Kennzeichnens von für eine sekundäre Ausgabeeinheit verschlüsselten Nachrichten, des kabellosen unidirektionalen Übertragens mittels einer bestimmten kabellosen Datenübertragungstechnologie und eines entsprechenden Kommunikationsprotokolls, sowie des potenziellen Sendens und Empfangens von Nachrichten auf der primären Ausgabeeinheit von und zu anderen Endgeräten, verantwortlich.

Entsprechend der beschriebenen Ausführungsvarianten des Verfahrens kann auch dieses Computerprogrammprodukt E in seinem Funktionsumfang sehr unterschiedlich umfangreich ausgestaltet sein. Insbesondere kann das Computerprogrammprodukt E in seiner Ausführung sehr unterschiedlich sein, je nachdem ob die Schritte (S01) und (S07), wie

bereits beschrieben, mittels Add-Ins in existierende Kommunikationsapplikationen oder mittels einer eigenen Kommunikationsapplikation umgesetzt werden.

In einer bevorzugten Ausführung des Computerprogrammprodukts E wird das Kommunikationsprotokoll, welches die genauen Regeln der kabellosen Datenübertragung von der primären Ausgabeeinheit zur sekundären Ausgabeeinheit bestimmt, innerhalb des Computerprogrammprodukts E verschlüsselt, um eine weitere Hürde einzubauen, die Angreifern für die Manipulation der Datenübertragung zur sekundären Ausgabeeinheit im Weg steht. In einer besonders bevorzugten Ausführung wird dieses verschlüsselte Kommunikationsprotokoll nur bei Bedarf mittels einer Nutzerauthentifizierung mittels Passworts abgerufen und entschlüsselt. In einer besonders bevorzugten Ausführung wird dieses Kommunikationsprotokoll regelmäßig verändert, sodass eine Kenntnis des Protokolls für den Angreifer nur kurzzeitig einen Angriffsvektor bietet.

Dem Fachmann erschließt sich die Existenz zweier zur Erfindung gehöriger Computerprogrammprodukte durch die Existenz sowohl der primären Ausgabeeinheit als auch der sekundären Ausgabeeinheit im Verfahren. Um diesen Zusammenhang zu verdeutlichen, wird nachfolgend auch das gesamte System zusammengehörigen Erfindung beschrieben.

Die vorliegende Erfindung betrifft zudem ein System, welches die Gesamtheit der Erfindung beschreibt und sowohl das erfindungsgemäße Verfahren als auch die sekundäre Ausgabeeinheit, als auch die Computerprogrammprodukte S und E, umfasst. Es sei explizit erwähnt, dass die primäre Ausgabeeinheit, welche Komponenten zum Speichern und Ausführen des Computerprogrammprodukts E umfasst, nicht zum System gehört, da die primäre Ausgabeeinheit als weitgehend beliebiges, allgemeines Mittel zur Datenverarbeitung zu verstehen ist. Das Computerprogrammprodukt E auf der primären Ausgabeeinheit ist in seiner Ausführung der Schritte S01, S02 und S07 für das erfindungsgemäße Verfahren dennoch essenziell. Primäre Ausgabeeinheit und sekundäre Ausgabeeinheit sowie Computerprogrammprodukt S und E sind durch die Verfahrensschritte des erfindungsgemäßen Verfahrens sowie durch Sender, Empfänger und die unidirektionale Ausgangsverbindung funktional miteinander verbunden, sodass alle Teile des Systems zur Erfindung zugehörig und für die Erfindung notwendig sind.

Abschließend sei angemerkt, dass sämtlichen Merkmalen, die in den Anmeldungsunterlagen und insbesondere in den abhängigen Ansprüchen genannt sind, trotz des vorgenommenen

formalen Rückbezugs auf einen oder mehrere bestimmte Ansprüche, auch einzeln oder in beliebiger Kombination eigenständiger Schutz zukommen soll.

Weitere Vorteile, Merkmale und Anwendungsmöglichkeiten der vorliegenden Erfindung ergeben sich auch aus der nachfolgenden Beschreibung von Ausführungsbeispielen und den Zeichnungen. Dabei bilden alle beschriebenen und/oder bildlich dargestellten Merkmale für sich oder in beliebiger Kombination den Gegenstand der vorliegenden Erfindung, auch unabhängig von ihrer Zusammenfassung in den Ansprüchen oder deren Rückbezügen.

Dabei können die in den Ansprüchen und in der Beschreibung erwähnten Merkmale jeweils einzeln für sich oder in beliebiger Kombination erfindungswesentlich sein.

Zudem ist darauf hinzuweisen, dass der Fachmann zweifelsohne erkennt, dass sich die einzelnen Merkmale, die in den vorstehenden konkreten Ausführungsformen beschrieben sind, auf angemessene Weise miteinander kombinieren lassen, soweit kein Widerspruch vorliegt, wobei zum Vermeiden unnötiger Wiederholung auf eine separate Beschreibung verschiedener möglicher Kombinationen verzichtet wird.

Je nach bestimmten Implementierungsanforderungen können Ausführungsbeispiele der Erfindung in Hardware oder in Software implementiert sein. Die Implementierung kann unter Verwendung eines digitalen Speichermediums, beispielsweise einer Floppy-Disk, einer DVD, einer Blu-Ray Disc, einer CD, eines ROM, eines PROM, eines EPROM, eines EEPROM oder eines FLASH-Speichers, einer Festplatte oder eines anderen magnetischen oder optischen Speichers durchgeführt werden, auf dem elektronisch lesbare Steuersignale gespeichert sind, die mit einer programmierbaren Hardwarekomponente derart zusammenwirken können oder zusammenwirken, dass das jeweilige Verfahren durchgeführt wird.

Eine Recheneinheit kann durch einen Prozessor, einen Computerprozessor (CPU = Central Processing Unit), einen Grafikprozessor (GPU = Graphics Processing Unit), einen Computer, ein Computersystem, einen anwendungsspezifischen integrierten Schaltkreis (ASIC = Application-Specific Integrated Circuit), einen integrierten Schaltkreis (IC = Integrated Circuit), ein Ein-Chip-System (SOC = System on Chip), ein programmierbares Logikelement oder ein feldprogrammierbares Gatterarray mit einem Mikroprozessor (FPGA = Field Programmable Gate Array) gebildet sein.

Allgemein können Ausführungsbeispiele der vorliegenden Erfindung als Programm, Firmware, Computerprogramm oder Computerprogrammprodukt mit einem Programmcode oder als Daten implementiert sein, wobei der Programmcode oder die Daten dahin gehend wirksam ist bzw. sind, eines der Verfahren durchzuführen, wenn das Programm auf einem Prozessor oder einer programmierbaren Hardwarekomponente abläuft. Der Programmcode oder die Daten kann bzw. können beispielsweise auch auf einem maschinenlesbaren Träger oder Datenträger gespeichert sein. Der Programmcode oder die Daten können unter anderem als Quellcode, Maschinencode oder Bytecode sowie als anderer Zwischencode vorliegen.

AUSFÜHRUNGSBEISPIELE

Die oben beschriebenen Eigenschaften, Merkmale und Vorteile dieser Erfindung sowie die Art und Weise, wie diese erreicht werden, werden klarer und deutlicher verständlich im Zusammenhang mit den folgenden Zeichnungen und Beschreibungen der Grundprinzipien und Ausführungsbeispiele der vorliegenden Erfindung.

Dabei wird die vorliegende Erfindung näher erläutert, ohne die Erfindung auf diese Zeichnungen und Beschreibungen zu beschränken.

Sofern in dieser Anmeldung der Begriff "kann" verwendet wird, handelt es sich sowohl um die technische Möglichkeit als auch um die tatsächliche technische Umsetzung. In den einzelnen Figuren gezeigte und zu dem jeweiligen Beispiel beschriebene Merkmale sind nicht auf das jeweilige Einzelbeispiel beschränkt. Der Singular schließt den Plural ein, es sei denn, aus dem Kontext geht eindeutig etwas anderes hervor.

Im Folgenden zeigt:

Fig. 1: den grundsätzlichen Kommunikationsprozess, wenn eine besonders sensible, und daher für eine sekundäre Ausgabeeinheit (2.2) verschlüsselte erste Nachricht (1.1) zwischen zwei Endgeräten, insbesondere primären Ausgabeeinheiten (2.1), versendet wird.

Fig. 2: die Verbindung und den Datenaustausch zwischen einer primären Ausgabeeinheit (2.1) und einer sekundären Ausgabeeinheit (2.2).

Fig. 3: Eine spezifische Ausführungsform der sekundären Ausgabeeinheit (2.2), bei der diese am seitlichen Gehäuse Anschlüsse für externe Speicherkarten (2.9) umfasst.

Die **Fig. 1** zeigt den grundsätzlichen Kommunikationsprozess, wenn eine besonders sensible, und daher für eine sekundäre Ausgabeeinheit (2.2) verschlüsselte erste Nachricht (1.1) zwischen zwei primären Ausgabeeinheit (2.1) versendet wird. Der Nutzer der ersten primären Ausgabeeinheit, der auf der linken Seite des Prozesses die unverschlüsselte Nachricht A (1.2) eingibt, nutzt hierfür eine sekundäre Ausgabeeinheit (2.2). Mithilfe einer spezifischen Verschlüsselungsart (1.3) wird aus der unverschlüsselten Nachricht A (1.2) eine verschlüsselte Nachricht A (1.1). Die primären Ausgabeeinheiten (2.1) des Senders und des Empfängers sowie das unsichere Netzwerk (2.3) verarbeiten ausschließlich die

verschlüsselte Nachricht A (1.1). Der Empfänger benötigt zum Entschlüsseln wiederum eine sekundäre Ausgabeeinheit (1.2) mit der spezifischen Verschlüsselungsart (1.3) (der Begriff wird hier für die Gesamtheit der Verschlüsselungstechnologie zum Ver- und Entschlüsseln verwendet). In der hier dargestellten Ausführung kombiniert die spezifische Verschlüsselungsart (1.3) jeweils zwei geheime Schlüssel, darunter einen kryptografischen Schlüssel (1.4), der auf einem Speichermedium der sekundären Ausgabeeinheit gespeichert ist, und einen externen Schlüssel (1.6), der auf einer externen Speicherkarte (1.5) gespeichert ist. Dies entspricht den Merkmalen der Erfindung nach Anspruch 8 und 15. In der dargestellten Ausführung wird ein symmetrisches kryptographisches Verfahren nach den Merkmalen von Anspruch 10 umgesetzt, in dem die Schlüssel zum Ent- und Verschlüsseln der Nachricht identisch sind. Neben diesen zwei speziellen Ausführungsformen zeigt die Figur 1 den generellen Informationsfluss im Sinne der Erfindung.

Fig. 2 zeigt die Verbindung und den Datenaustausch zwischen einer primären Ausgabeeinheit (2.1) und einer sekundären Ausgabeeinheit (2.2). Die primäre Ausgabeeinheit, in diesem Beispiel als Smartphone dargestellt, sendet eine verschlüsselte Nachricht mittels einer kabellosen Datenübertragungstechnologie (2.6) an die sekundäre Ausgabeeinheit (2.2). Die genaue Technologie, sowie Sender und Empfänger, sind in dieser Figur nicht genauer definiert. Mithilfe eines Ausgabemittels (2.4), in dieser Ausführung ein Display, kann eine Nachricht dargestellt, mithilfe des Eingabemittels (2.5) eine Nachricht verfasst werden. Verfasste Nachrichten, die versendet werden sollen, werden mithilfe einer unidirektionalen Datenverbindung (2.7) an die primäre Ausgabeeinheit übertragen, die in dieser Darstellung als unidirektionale Kabelverbindung (2.8) nach Anspruch 13 ausgeführt ist. In dieser speziellen Ausführungsvariante ist die sekundäre Ausgabeeinheit (2.2) nach gleichen Außenmaßen wie die primäre Ausgabeeinheit (2.1) gestaltet, wodurch vorteilhaft eine zueinander fehlerfreie Ausrichtung und uniforme Handhabung, durch eine parallele Ausrichtung aller Außenkanten beider Geräte erreicht werden kann, wobei in der Darstellung keine konkreten Verbindungselemente nach Anspruch 17 ausgeführt werden. Neben den speziellen Ausführungsformen bezüglich der Form der sekundären Ausgabeeinheit (2.2) sowie der unidirektionalen Kabelverbindung (2.8) zeigt die Figur 2 generelle Komponenten der sekundären Ausgabeeinheit sowie das Verbindungsprinzip zur primären Ausgabeeinheit (2.1).

Fig. 3 zeigt eine bevorzugte Ausführungsform der sekundären Ausgabeeinheit (2.2), bei der diese am seitlichen Gehäuse Anschlüsse für externe Speicherkarten (2.9) umfasst. Die Anzahl von drei Anschlüssen für externe Speicherkarten ist hier eine mögliche, aber keine besonders bevorzugte Ausführungsform. Diese Ausführungsform nach Anspruch 15 erlaubt

es, in die spezifische Verschlüsselungsart (1.3) einen geheimen, externen Schlüssel (1.6) auf einer externen Speicherkarte (1.5) einzubeziehen, sodass Nachrichten nur von solchen sekundären Ausgabeeinheiten entschlüsselt werden können, die außerdem über einen solchen externen Schlüssel verfügen (siehe Fig.1).

Es ist zu beachten, dass Elemente oder Merkmale, die in Struktur und/oder Funktion ähnlich sind, in verschiedenen Ausführungsformen mit den gleichen Bezugszeichen bezeichnet werden. Wenn also ein bestimmtes Merkmal nicht im Detail unter Bezugnahme auf eine bestimmte Ausführungsform beschrieben wird, kann eine Beschreibung dieses Merkmals aus der Beschreibung einer anderen Ausführungsform übernommen werden.

Obwohl die Erfindung unter Bezugnahme auf bestimmte Ausführungsbeispiele beschrieben und illustriert wurde, soll die Erfindung nicht auf diese Ausführungsbeispiele beschränkt werden. Der Fachmann erkennt, dass Variationen und Modifikationen vorgenommen werden können, ohne dass der wahre Umfang der Erfindung, wie er durch die Ansprüche und Beschreibung definiert ist, verlassen wird. Es ist daher beabsichtigt, im Rahmen der Erfindung alle Variationen und Modifikationen, die in den Anwendungsbereich der beigefügten Ansprüche und deren Äquivalente fallen, einzuschließen.

BEZUGSZEICHENLISTE

(1.1) Verschlüsselte erste Nachricht

(1.2) Unverschlüsselte erste Nachricht

(1.3) Spezifische Verschlüsselungsart

(1.4) Kryptografischer Schlüssel

(1.5) Externe Speicherkarte

(1.6) Externer Schlüssel

(2.1) Endgerät, insbesondere primäre Ausgabeeinheit

(2.2) sekundäre Ausgabeeinheit

(2.3) Unsicheres Netzwerk

(2.4) Ausgabemittel

(2.5) Eingabemittel

(2.6) Kabellose Datenübertragungstechnologie

(2.7) Unidirektionale Ausgangsverbindung

(2.8) Unidirektionale Kabelverbindung

(2.9) Anschlüsse für Speicherkarten

PATENTANSPRÜCHE

1. **Verfahren** zum Ausgeben und Kommunizieren verschlüsselter elektronischer Daten, umfassend die Schritte:

   - Identifizieren (S01) einer verschlüsselten ersten Nachricht (1.1) auf einer primären Ausgabeeinheit (2.1),
     wobei die verschlüsselte erste Nachricht (1.1) mit einer spezifischen Verschlüsselungsart (1.3) verschlüsselt worden ist, und
     wobei die verschlüsselte erste Nachricht (1.1) nur mithilfe einer sekundären Ausgabeeinheit (2.2) entschlüsselt werden kann,

   - unidirektionales Übertragen (S02) der verschlüsselten ersten Nachricht (1.1) von der primären Ausgabeeinheit (2.1) auf die sekundäre Ausgabeeinheit (2.2),
     wobei das unidirektionale Übertragen (S02) mittels elektromagnetischer Wellen, vorzugsweise optoelektronisch, mittels Schallwellen und/oder mittels Vibrationen erfolgt,

   - Entschlüsseln (S03) der empfangenen ersten verschlüsselten Nachricht (1.1) auf der sekundären Ausgabeeinheit (2.2), wobei das Entschlüsseln mittels zumindest einem von der sekundären Ausgabeeinheit (2.2) umfassten kryptografischen Schlüssels (1.4) erfolgt,

   - Ausgeben (S04) der resultierenden entschlüsselten ersten Nachricht (1.2) auf der sekundären Ausgabeeinheit (2.2),

   - Eingeben und Verschlüsseln (S05) einer unverschlüsselten zweiten Nachricht auf der sekundären Ausgabeeinheit (2.2), wobei das Verschlüssein der unverschlüsselten zweiten Nachricht eine verschlüsselte zweite Nachricht erzeugt,

   - unidirektionales Übertragen (S06) der verschlüsselten zweiten Nachricht von der sekundären Ausgabeeinheit (2.2) auf die primäre Ausgabeeinheit (2.1) mittels einer zur sekundäre Ausgabeeinheit (2.2) zugehörigen unidirektionalen Ausgangsverbindung (2.7/2.8),

   - Entschlüsseln und Ausgeben (S07) der verschlüsselten zweiten Nachricht auf der primären Ausgabeeinheit (2.1).

2. Verfahren nach Anspruch 1, wobei der Schritt des Kennzeichnens (S01) sowie der Schritt des Ausgebens und Kennzeichnens (S06) mithilfe von Add-Ins innerhalb von ausgewählten, vorhandenen Kommunikationsanwendungen der primären Ausgabeeinheit (2.1) stattfindet.

3. Verfahren nach Anspruch 1 oder 2, wobei der Schritt des Kennzeichnens (S01) sowie der Schritt des Ausgebens und Kennzeichnens (S06) innerhalb einer eigenen Kommunikationsapplikation der primären Ausgabeeinheit (2.1) umgesetzt wird, wobei der Schritt des Kennzeichnens (S01) zusätzlich das Empfangen von Nachrichten umfasst, wobei der Schrit des Ausgebens und Kennzeichnens (S06) zusätzlich das Versenden von Nachrichten umfasst.

4. Verfahren nach einem der Ansprüche 1 bis 3, wobei zumindest im Schritt des Entschlüsselns (S04) zusätzlich zu dem zur sekundären Ausgabeeinheit (2.2) gehörenden geheimen kryptografischen Schlüssel (1.4) zumindest ein geheimer externer Schlüssel (1.6) verwendet wird.

5. Verfahren nach Anspruch 4, wobei der externe geheime Schlüssel (1.7) auf einem externen Speichermedium (1.5) gespeichert ist.

6. Verfahren nach einem der Ansprüche 1 bis 5, wobei der Schritt des Entschlüsseln (S04) und/oder der Schritt des Verschlüsselns (S05) mithilfe asymmetrischer kryptographischer Verfahren umgesetzt werden.

7. Verfahren nach einem der Ansprüche 1 bis 6, wobei der Schritt des Entschlüsseln (S04) und/oder der Schritt des Verschlüsselns (S05) mithilfe symmetrischer kryptographischer Verfahren umgesetzt werden.

8. Verfahren nach einem der Ansprüche 1 bis 7, wobei der Schritt des Entschlüsseln (S04) zusätzlich das Prüfen einer digitalen Signatur umfasst und/oder der Schrit des Verschlüsselns (S05) zusätzlich das Hinzufügen einer digitalen Signatur umfasst.

9. **Sekundäre Ausgabeeinheit** (2.2), umfassend zumindest die folgenden Komponenten:
   - ein Empfangsmittel, das für den Schritt des unidirektionalen Übertragens (S02), insbesondere für eine kabellose Datenübertragungstechnologie, mittels elektromagnetischer Wellen, vorzugsweise optoelektronisch, mittels Schallwellen und/oder mittels Vibrationen zum unidirektionalen Empfangen einer

verschlüsselten ersten Nachricht (1.1) von einer primären Ausgabeeinheit (2.1) eingerichtet ist,

- eine Recheneinheit, die zum Entschlüsseln (S03) der empfangenen ersten verschlüsselten Nachricht (1.1) eingerichtet ist, wobei das Entschlüsseln vorzugsweise mittels zumindest einem von der sekundären Ausgabeeinheit (2.2) umfassten kryptografischen Schlüssels (1.4) erfolgt,
- Eingeben und Verschlüsseln (S05) einer unverschlüsselten zweiten Nachricht auf der sekundären Ausgabeeinheit (2.2), wobei das Verschlüssein der unverschlüsselten zweiten Nachricht eine verschlüsselte zweite Nachricht erzeugt,
- ein Ausgabemittel (2.4), das zum unidirektionalen Übertragen (S06) einer verschlüsselten zweiten Nachricht auf eine primäre Ausgabeeinheit (2.1) eingerichtet ist, insbesondere mittels einer zur sekundäre Ausgabeeinheit (2.2) zugehörigen unidirektionalen Ausgangsverbindung,
  wobei das Ausgabemittel vorzugsweise ein Display ist, Eingabemittel (2.5), Empfänger für einer unidirektionalen Übertragung, insbesondere für ein kabellose Datenübertragungstechnologie, unidirektionales Ausgangsmittel (2.7), Speichermedium, und Rechenmedium.

10. Sekundäre Ausgabeeinheit nach Anspruch 9, wobei das unidirektionale Ausgangsmittel (2.7) mittels einer unidirektionalen Ausgangsverbindung, insbesondere mittels einer unidirektionalen Kabelverbindung (2.8), zwischen der primären Ausgabeeinheit (2.1) und der sekundären Ausgabeeinheit (2.2) realisiert ist.

11. Sekundäre Ausgabeeinheit nach Anspruch 9 oder 10, wobei der Empfänger für eine unidirektionalen Übertragung als kabellose Datenübertragungstechnologie entsprechend der verwendeten kabellosen Datenübertragungstechnologie (2.6) in einem der Ansprüche 4 bis 6 ausgestaltet ist.

12. Sekundäre Ausgabeeinheit nach einem der Ansprüche 9 bis 11, wobei die Vorrichtung zumindest einen Anschluss für eine Speicherkarte (2.9) umfasst, wodurch insbesondere das Verfahren mit den Merkmalen der Ansprüche 7 und 8 ermöglicht ist.

13. Sekundäre Ausgabeeinheit nach Anspruch 12, wobei die Anschlüsse für Speicherkarten (2.9) so ausgestaltet sind, dass eingefügte Speicherkarten nicht zerstörungsfrei entnommen werden können.

14. Sekundäre Ausgabeeinheit nach einem der Ansprüche 9 bis 13, ferner aufweisend zumindest ein Verbindungselement, das derart eingerichtet ist, die sekundäre Ausgabeeinheit physisch an die primären Ausgabeeinheit (2.1) zu koppeln, wobei durch das Koppeln Sender und Empfänger der kabellosen Datenübertragungstechnologie (2.6) bezüglich der Kommunikation fehlerfrei zueinander ausgerichtet sind und außerdem beide Geräte durch den Nutzer uniform gehandhabt werden können.

15. **Computerprogrammprodukt S**, das auf dem Speichermedium der sekundäre Ausgabeeinheit (2.2) nach einem der Ansprüche 9 bis 14 gespeichert ist und bei Ausführung durch ein Rechenmedium der sekundären Ausgabeeinheit diese zur Durchführung zumindest der Schritte (S03), (S04), (S05) und (S06) des Verfahrens nach Anspruch 1 oder einem der Ansprüche 2 bis 8 veranlasst.

16. **Computerprogrammprodukt E**, das auf einem Speichermedium der primären Ausgabeeinheit (2.1) gespeichert ist und bei Ausführen die primäre Ausgabeeinheit (2.1) zur Durchführung zumindest der Schritte S01, S02 und S07 nach einem der Ansprüche 1 bis 3 veranlasst.

17. **System** zur Implementierung des Verfahrens nach einem der Ansprüche 1 bis 8, umfassend die sekundäre Ausgabeeinheit (2.2) nach einem der Ansprüche 9 bis 14, ein Computerprogrammprodukt S nach Anspruch 15, sowie ein Computerprogrammprodukt E nach Anspruch 16.

LU103080

FIGUREN

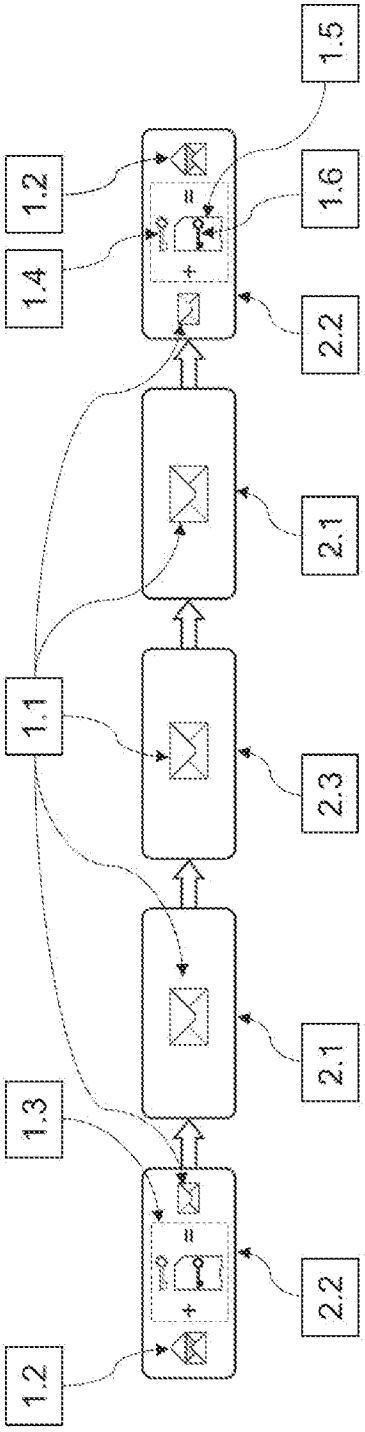

Fig. 1

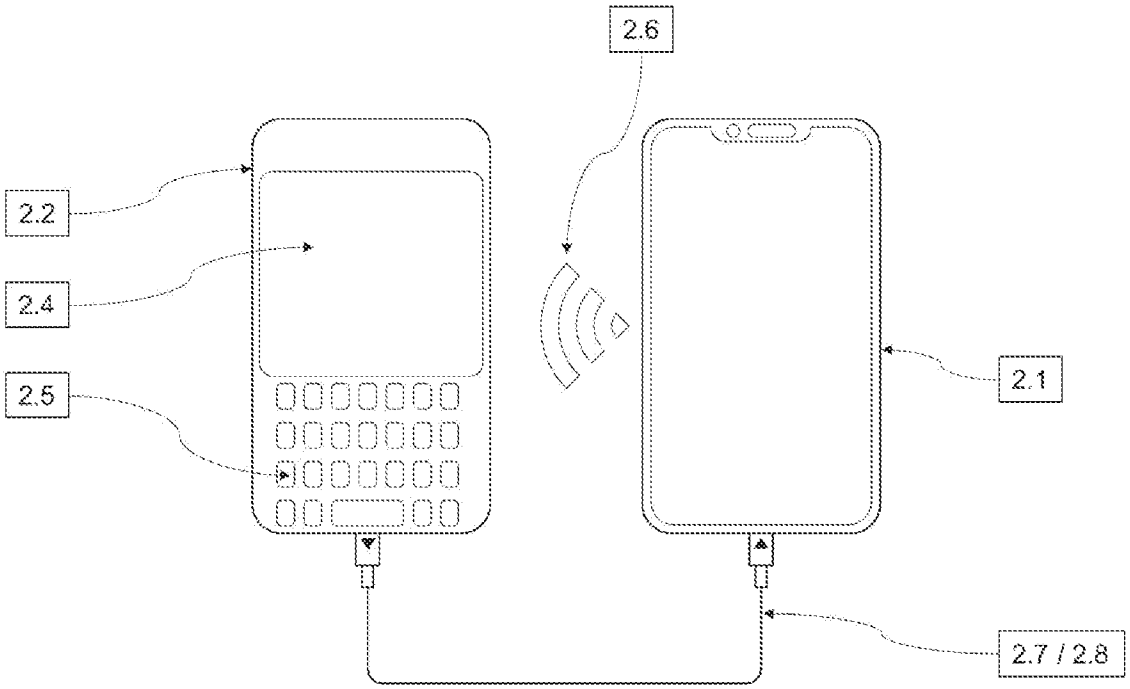

Fig. 2

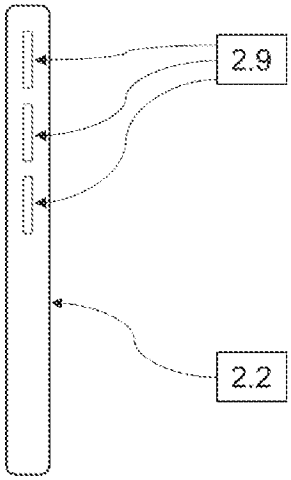

Fig. 3