(19) Deutsches Patent- und Markenamt

(10) **DE 10 2019 220 220 A1** 2021.06.24

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2019 220 220.9**
(22) Anmeldetag: **19.12.2019**
(43) Offenlegungstag: **24.06.2021**

(51) Int Cl.: ***G06F 21/62*** (2013.01)
G07C 5/00 (2006.01)

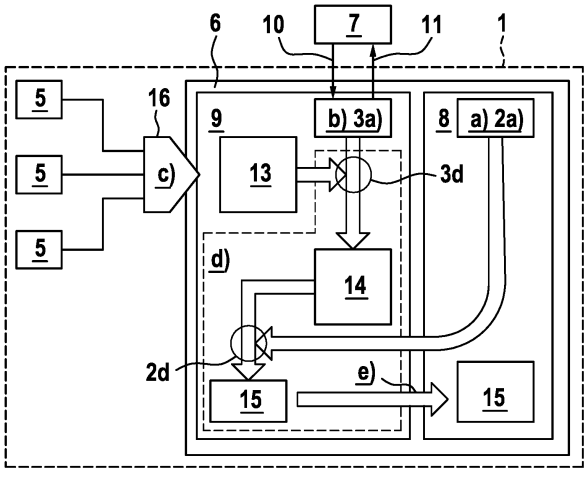
(71) Anmelder:
Robert Bosch GmbH, 70469 Stuttgart, DE

(72) Erfinder:
Hoffmann, Sebastian, 74321 Bietigheim-Bissingen, DE; Breitbart, Jens, 36208 Wildeck, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **Verfahren zur Speicherung von Betriebsdaten eines Kraftfahrzeuges**

(57) Zusammenfassung: Verfahren zur Speicherung von Betriebsdaten, die während eines Betriebs des Kraftfahrzeuges (1) mit einem Fahrzeugführer entstehen, wobei die Betriebsdaten bei der Speicherung derart verschlüsselt werden, dass zum Entschlüsseln der Betriebsdaten eine Mitwirkung des Fahrzeugführers des Kraftfahrzeugs (1) erforderlich ist.



Beschreibung

Stand der Technik

[0001] Betriebsdatenrekorder zum Speichern von Betriebsdaten des Betriebs eines Kraftfahrzeuges sind an sich bekannt. Es ist auch bekannt Fotos oder Kameraaufnahmen, die während oder nach einem Unfall eines Kraftfahrzeuges entstanden sind, zu speichern. Betriebsdaten und insbesondere derartige Fotos oder Kameraaufnahmen sind für Versicherungsfirmen außerordentlich interessant, um den Schuldigen eines Unfalles zu ermitteln. Mit derartigen Daten kann der Hergang eines Unfalls gegebenenfalls rekonstruiert werden.

[0002] Die Idee Betriebsdaten und insbesondere Fotos oder Kameraaufnahmen zu verschlüsseln, um sie vor unberechtigten Zugriffen zu schützen ist ebenfalls bekannt. Ein erhebliches Problem im Zusammenhang mit der Speicherung derartiger Daten sind Datenschutzbestimmungen und Datenschutzinteressen des Kraftfahrzeugbetreibers, des Kraftfahrzeugherstellers und des Fahrzeugführers des Kraftfahrzeuges. Datenschutzbestimmungen sind in verschiedenen Ländern zusätzlich noch verschieden, sodass sehr unterschiedliche Regulierung in diesem Zusammenhang eingehalten werden müssen, wenn ein universell einsetzbares Speichersystem für Betriebsdaten bereitgestellt werden soll.

[0003] In besonderer Weise problematisch ist es, wenn derartige Daten in der Sphäre eines Kraftfahrzeugherstellers gespeichert werden und dadurch nur der Kraftfahrzeughersteller über die Herausgabe derartiger Daten entscheiden kann. Insbesondere im Zusammenhang mit den autonom fahrenden Fahrzeugen liegt die Verantwortung für Verkehrsunfälle regelmäßig entweder beim Fahrzeugführer des Kraftfahrzeuges oder beim Hersteller des Kraftfahrzeuges, je nachdem welcher Fehler wann und wie eingetreten ist und für den Verkehrsunfall ursächlich war. In derartigen Situationen ist es für den Fahrzeugführer eines Kraftfahrzeuges extrem schwierig, seine Interessen zu vertreten, weil die notwendigen Daten zur Aufklärung der Verantwortung eines Unfalls vom Hersteller zurückgehalten werden könnten.

[0004] Bei Unfällen mit autonom betreibbaren Kraftfahrzeugen ist beispielsweise oft zu klären, ob der Fahrzeugführer in einer Gefahrensituation rechtzeitig die Kontrolle über das Fahrzeug übernommen hat oder sich in unzulässiger Art und Weise auf den autonomen Betrieb des Fahrzeuges verlassen hat. In einer derartigen Situation sind umfangreiche aufgezeichnete Betriebsdaten extrem hilfreich.

Offenbarung der Erfindung

[0005] Ausgehend von dieser Situation soll hier ein Verfahren zur Speicherung von Betriebsdaten eines Kraftfahrzeugs beschrieben werden, welches dazu geeignet ist, einen Zugriff auf Daten im Bedarfsfall zu ermöglichen, Manipulationssicherheit der Daten zu gewährleisten und gleichzeitig kompatibel zu geltenden Vertraulichkeitsinteressen, Vertraulichkeitsbestimmungen und Datenschutzbestimmungen zu sein.

[0006] Die Erfindung betrifft ein Verfahren zur Speicherung von Betriebsdaten, die während eines Betriebs des Kraftfahrzeuges mit einem Fahrzeugführer entstehen, wobei die Betriebsdaten bei der Speicherung derart verschlüsselt werden, dass zum Entschlüsseln der Betriebsdaten eine Mitwirkung des Fahrzeugführers des Kraftfahrzeugs erforderlich ist.

[0007] Dies bedeutet, dass die Betriebsdaten so verschlüsselt werden, dass ohne eine Mitwirkung des Fahrzeugführers des Kraftfahrzeugs keine Entschlüsselung der Betriebsdaten möglich ist. Ein Fahrzeugführer behält also trotz der Speicherung der Betriebsdaten die Kontrolle über die Verwertung der Betriebsdaten.

[0008] Die Erfindung betrifft ein Verfahren zur Speicherung von Betriebsdaten eines Kraftfahrzeuges aufweisend die folgenden Schritte:

a) Ermitteln eines ersten öffentlichen Schlüssels eines ersten Schlüsselpaars, dessen erster geheimer Schlüssel in einer ersten geschützten Sphäre einer für den technischen Betrieb des Kraftfahrzeugs verantwortlichen Stelle ist,

b) Ermitteln eines zweiten öffentlichen Schlüssels eines zweiten Schlüsselpaars, dessen geheimer Schlüssel in einer zweiten geschützten Sphäre eines Fahrzeugführers des Kraftfahrzeugs ist,

c) Akquirieren von Betriebsdaten des Kraftfahrzeuges während eines Betriebs des Kraftfahrzeuges,

d) Verschlüsseln der Betriebsdaten mit dem ersten öffentlichen Schlüssel und dem zweiten öffentlichen Schlüssel,

e) Ablegen der verschlüsselten Betriebsdaten auf einem Datenspeicher.

[0009] Das erste Schlüsselpaar mit dem ersten öffentlichen Schlüssel und dem ersten geheimen Schlüssel sowie das zweite Schlüsselpaar mit dem zweiten öffentlichen Schlüssel und dem zweiten geheimen Schlüssel sind jeweils übliche Schlüsselpaare für ein asymmetrisches Verschlüsselungsverfahren. In solchen Verfahren ist es möglich, mit dem öffentlichen Schlüssel des jeweiligen Schlüsselpaars

Daten zu verschlüsseln. Eine Entschlüsselung der Daten ist nur möglich, wenn auch der geheime Schlüssel des jeweiligen Schlüsselpaars zur Verfügung steht. Der geheime Schlüssel des jeweiligen Schlüsselpaars wird in einer geschützten Sphäre aufbewahrt.

[0010] Die theoretische Grundlage für asymmetrische Verschlüsselungsverfahren sind Falltürfunktionen, also Funktionen, die leicht zu berechnen sind, aber ohne ein Geheimnis praktisch unmöglich zu invertieren sind. Der geheime Schlüssel ist dann eine Beschreibung der Funktion, der öffentliche Schlüssel ist die Falltür. Mit der Anwendung des öffentlichen Schlüssels auf die zu verschlüsselnden Daten, kann aus den zu verschlüsselnden Daten eine Menge an verschlüsselten Daten zu stehen, die ohne den geheimen Schlüssel wertlos sind. Eine Voraussetzung ist natürlich, dass der private Schlüssel aus dem öffentlichen nicht berechnet werden kann.

[0011] Asymmetrische Verschlüsselungsverfahren bzw. Falltürfunktionen können beispielsweise auf einem der folgenden mathematischen Verfahren basieren:

- elliptische Kurven,
- RSA-Verfahren,
- PGP-Verfahren

[0012] Wie weiter oben beschrieben, ist der erste geheime Schlüssel in einer geschützten Sphäre eines für den technischen Betrieb des Kraftfahrzeugs Verantwortlichen aufbewahrt. Ein solcher für den technischen Betrieb des Kraftfahrzeuges Verantwortlicher kann beispielsweise der Hersteller des Kraftfahrzeuges sein, welcher für die korrekte Funktionsweise des Kraftfahrzeuges und insbesondere der Systeme des Kraftfahrzeuges zum autonomen Fahren verantwortlich ist und gegebenenfalls auch haftbar gemacht werden kann, wenn bestimmte Funktionen des Kraftfahrzeuges nicht ordnungsgemäß funktionieren. Ein solcher für den technischen Betrieb des Kraftfahrzeuges Verantwortlicher kann aber auch eine andere Stelle sein, die zumindest gegenüber dem Fahrzeugführer des Kraftfahrzeuges eine gewisse Verantwortung für die Betriebssicherheit des Kraftfahrzeuges und seiner Systeme aufweist. Ein Beispiel für so jemanden ist doppelt? (s. Satzanfang) ein Mietwagenbetreiber oder eine ähnliche Stelle. Für die Durchführung des beschriebenen Verfahrens wird der erste geheime Schlüssel nicht benötigt bzw. der erste geheime Schlüssel muss für die Durchführung des beschriebenen Verfahrens nicht vorliegen. Die geschützte Sphäre kann daher vollkommen unabhängig von dem Kraftfahrzeug selbst sein. Bevorzugt ist dies auch tatsächlich so eingerichtet. Bei der geschützten Sphäre kann es sich beispielsweise um einen Computerserver beim Hersteller des Kraftfahrzeuges oder bei einem Mietwagenbetreiber handeln.

[0013] Wie weiter oben beschrieben, ist der zweite geheime Schlüssel in einer zweiten geschützten Sphäre eines Fahrzeugführers des Kraftfahrzeuges aufbewahrt. Eine zweite geschützte Sphäre des Fahrzeugführers des Kraftfahrzeugs kann beispielsweise ein Mobiltelefon im Besitz des Fahrzeugführers des Kraftfahrzeuges oder gegebenenfalls auch eine elektronische Signaturkarte des Fahrzeugführers des Kraftfahrzeuges oder ein ähnliches Gerät sein. Es ist auch möglich, dass die zweite geschützte Sphäre des Fahrzeugführers ein Computer oder ein Netzwerkspeicher oder eine ähnliche Komponente ist, welche unter der Kontrolle des Fahrzeugführers steht. Für die Durchführung des beschriebenen Verfahrens ist es regelmäßig nicht erforderlich, dass der zweite geheime Schlüssel während der Durchführung des Verfahrens vorliegt. Daher kann die zweite Sphäre auch vollkommen losgelöst von dem Kraftfahrzeug sein. Es ist nicht erforderlich, dass die technische Einheit, die die zweite geschützte Sphäre bildet, sich in dem Kraftfahrzeug selbst befindet. In vielen Fällen ist dies aber auch nicht schädlich. Beispielsweise ist dies bei einem Mobiltelefon oder einer Signaturkarte möglich, welche die zweite geschützte Sphäre bereitstellen kann und die ein Fahrzeugführer des Kraftfahrzeuges in das Kraftfahrzeug mitnehmen kann. Es ist technisch möglich, beispielsweise in ein Mobiltelefon oder einer Signaturkarte einen geheimen Schlüssel für das beschriebene Verfahren sicher zu lagern, wenn das Mobiltelefon hardwaretechnisch und/oder softwaretechnisch entsprechend eingerichtet ist.

[0014] Das Ermitteln des ersten öffentlichen Schlüssels in Schritt a) und des zweiten öffentlichen Schlüssels in Schritt b) kann das Auslesen des jeweiligen Schlüssels aus einem Speicher umfassen. Es können allerdings auch weitere Unterschritte zum Ermitteln des Schlüssels aus externen Quellen ausgeführt werden. Hierzu werden später detailliertere Varianten ausgeführt.

[0015] Das Akquirieren von Betriebsdaten des Kraftfahrzeuges in Schritt c) umfasst insbesondere das Empfangen von verschiedenen Sensordaten von verschiedenen Sensoren in dem Kraftfahrzeug über eine Datenschnittstelle eines Betriebsdatenrekorders.

[0016] Die in Schritt c) akquirierten Betriebsdaten werden anschließend in Schritt d) sowohl mit dem ersten öffentlichen Schlüssel als auch mit dem zweiten öffentlichen Schlüssel verschlüsselt. Bevorzugt umfasst dies die Durchführung von zwei aufeinanderfolgenden Verschlüsselungsschritten, wobei zunächst mit dem ersten öffentlichen Schlüssel oder dem zweiten öffentlichen Schlüssel und anschließend mit dem jeweils anderen Schlüssel die Verschlüsselung erfolgt. Das Ergebnis dieses Prozesses sind doppelt verschlüsselte Betriebsdaten. Die Reihenfolge der Verschlüsselung (zunächst die Ver-

schlüsselung mit dem ersten öffentlichen Schlüssel oder zunächst die Verschlüsselung mit dem zweiten öffentlichen Schlüssel) spielt für das hier beschriebene Verfahren keine entscheidende Rolle. Vielmehr entscheidend ist, dass das Verschlüsseln mit beiden öffentlichen Schlüsseln so durchgeführt wird, dass hinterher auch beide geheime Schlüssel benötigt werden, um eine Entschlüsselung der Daten durchzuführen. Es sind auch Kryptographieverfahren denkbar, bei welchen die Betriebsdaten jeweils abschnittsweise hintereinander mit dem ersten öffentlichen Schlüssel und dem zweiten öffentlichen Schlüssel verschlüsselt werden oder aber auch eine Verschlüsselung gleichzeitig mit beiden öffentlichen Schlüsseln erfolgt. Bei solchen Verfahren kann beispielsweise immer eine geringe Teildatenmenge der Betriebsdaten zunächst mit dem ersten öffentlichen Schlüssel und dann mit dem zweiten öffentlichen Schlüssel verschlüsselt werden. Gegebenenfalls kann die Reihenfolge der Verschlüsselung mit dem ersten öffentlichen Schlüssel und dem zweiten öffentlichen Schlüssel während des Betriebs regelmäßig geändert werden.

[0017] Das Ablegen der verschlüsselten Betriebsdaten auf einem Datenspeicher in Schritt e) erfolgt bevorzugt so, dass ein Zugriff auf diese Betriebsdaten möglich ist, wenn dieser Zugriff vorteilhaft und/oder erforderlich ist. Dies kann beispielsweise in dem Fall sein, wenn ein Unfall des Kraftfahrzeuges eingetreten ist und die Betriebsdaten zur Aufklärung dieses Unfalls verwendet werden sollen. Gegebenenfalls können die Betriebsdaten auch an mehreren Stellen abgelegt werden. Denkbar ist, dass sowohl ein Ablegen auf einem Speicher des Fahrzeugführers als auch ein Ablegen auf einem Speicher des für den technischen Betrieb des Kraftfahrzeugs Verantwortlichen erfolgt.

[0018] Das Verfahren ist besonders vorteilhaft, wenn die Betriebsdaten zumindest eine der folgenden Arten von Daten umfassen:

- Sensordaten von Sensoren zur Überwachung des Umfeldes des Kraftfahrzeugs,
- Sensordaten von Sensoren zur Überwachung des Innenraums des Kraftfahrzeugs,
- Messdaten, zur Überwachung von Insassen des Kraftfahrzeugs, und
- Kameraaufnahmen.

[0019] Die beschriebenen Arten von Betriebsdaten sind hier nicht abschließend. Es ist möglich, dass weitere Arten von Betriebsdaten aufgezeichnet werden. Insbesondere ist bevorzugt, dass mindestens zwei oder sogar mindestens drei verschiedene Arten von Betriebsdaten aufgezeichnet werden. Insbesondere im Zusammenhang mit Kameraaufnahmen und Messdaten zur Überwachung von Insassen des Fahrzeuges ist es erforderlich, dass Datenschutzbestimmungen eingehalten werden. Durch das beschriebene Verfahren und die Verschlüsselung mit dem zweiten öffentlichen Schlüssel ist sichergestellt, dass nur im Falle der Zustimmung des Fahrzeugführers des Kraftfahrzeuges ein Zugriff auf die Daten möglich ist.

[0020] Das Verfahren ist besonders vorteilhaft, wenn das Verfahren in einem Betriebsdatenrekorder des Kraftfahrzeuges durchgeführt wird.

[0021] Ein solcher Betriebsdatenrekorder ist üblicherweise nach Art eines Steuergerätes aufgebaut. Ein solcher Betriebsdatenrekorder kann auch als virtuellere Komponente in einem Hardware-Steuergerät realisiert sein, in welchem weitere Komponente realisiert sind. Das Hardware-Steuergerät stellt dann eine Virtualisierungsumgebung bereit, in der Hardware-Steuergeräte abgelegt und betreibbar sind.

[0022] Das Verfahren ist besonders vorteilhaft, wenn der Datenspeicher in dem Betriebsdatenrekorder des Kraftfahrzeugs angeordnet ist.

[0023] Der Datenspeicher ist insbesondere in einem nicht volatilen Speicher in dem Betriebsdatenrekorder realisiert. Bevorzugt sind die Daten in dem Betriebsdatenrekorder so abgelegt, dass eine Zerstörung der Daten durch einen Unfall vollständig oder zumindest weitestgehend verhindert ist. Der Aufbau des Betriebsdatenrekorders ist in diesem Zusammenhang bevorzugt ähnlich einer Blackbox ausgeführt.

[0024] Das Verfahren ist besonders vorteilhaft, wenn der Datenspeicher in einem von dem Kraftfahrzeug separaten elektronischen Gerät angeordnet ist.

[0025] Das Verfahren ist besonders vorteilhaft, wenn das elektronische Gerät ein mobiles Endgerät des Fahrzeugführers des Kraftfahrzeugs ist.

[0026] Der Datenspeicher kann insbesondere in einem transportablen elektronischen Gerät angeordnet sein, beispielsweise in einem Chip eines mobilen Endgerätes des Fahrzeugführers des Kraftfahrzeuges oder auch in einer Cloud. So kann der Fahrzeugführer des Kraftfahrzeuges die verschlüsselten Betriebsdaten unproblematisch sichern.

[0027] Mobile Endgeräte sind beispielsweise Mobiltelefone, Tablets oder ähnliche Komponenten. Die für das beschriebene Verfahren erforderlichen Funktionalitäten in einer Sphäre des Fahrzeugführers des Kraftfahrzeuges können mit derartigen mobilen Endgeräten einfach realisiert werden.

[0028] Verfahren nach einem der vorhergehenden Ansprüche, wobei der erste öffentliche Schlüssel des ersten Schlüsselpaars in Schritt a) aus einem nicht volatilen Speicher in dem Kraftfahrzeug ermittelt wird.

[0029] Ein nicht volatiler Speicher ist ein Speicher, aus dem dort einmal eingebrachte Daten nicht so einfach gelöscht werden können. Ein solcher nicht volatiler Speicher hat bevorzugt besondere Schutzmaßnahmen zur Vermeidung der Manipulation oder des Verlusts von dort eingebrachten Daten. Der erste öffentliche Schlüssel ist in dem Kraftfahrzeug bevorzugt fest hinterlegt. Der erste öffentliche Schlüssel kann beispielsweise bereits bei der Herstellung des Kraftfahrzeuges fest für dieses Kraftfahrzeug, in dem nicht volatilen Speicher in dem Kraftfahrzeug, hinterlegt sein. Der nicht volatile Speicher kann beispielsweise Bestandteil des Betriebsdatenrekorders sein. Der zugehörige erste geheime Schlüssel des ersten Schlüsselpaars wird bei der Herstellung des ersten öffentlichen Schlüssels vorzugsweise in der geschützten Sphäre des für den technischen Betrieb des Kraftfahrzeuges Verantwortlichen (beispielsweise in der Sphäre des Kraftfahrzeugherstellers) abgelegt.

[0030] Das Verfahren ist besonders vorteilhaft, wenn der zweite öffentliche Schlüssel des zweiten Schlüsselpaars in Schritt b) von einem separaten elektronischen Gerät bereitgestellt wird.

[0031] Insbesondere erfolgt also auch die Bereitstellung des zweiten öffentlichen Schlüssels über ein separates elektronisches Gerät oder von einem separaten elektronischen Gerät, welches (wie weiter oben schon beschrieben) ein mobiles Endgerät eines Fahrzeugführers des Kraftfahrzeuges sein kann. Auf diese Art und Weise ist der Schlüssel einfach austauschbar, wenn ein anderer Fahrzeugführer das Kraftfahrzeug betreibt. Dann werden Betriebsdaten eines Kraftfahrzeugbetriebs, der von einem ersten Fahrzeugführer durchgeführt wird, mit dem zweiten öffentlichen Schlüssel des ersten Fahrzeugführers und die Betriebsdaten eines Kraftfahrzeugbetriebs, der von einem zweiten Fahrzeugführer durchgeführt wird, mit dem zweiten öffentlichen Schlüssel des zweiten Fahrzeugführers verschlüsselt.

[0032] Das Verfahren ist besonders vorteilhaft, wenn der zweite öffentliche Schlüssel des zweiten Schlüsselpaars vor dem Start einer Betriebsphase des Kraftfahrzeugs in dem von dem Kraftfahrzeug separaten elektronischen Gerät generiert wird.

[0033] Bevorzugt befindet sich in dem separaten elektronischen Gerät eine Vorrichtung zur Generierung von öffentlichen Schlüsseln zu dem ersten geheimen Schlüssel. Auf diese Art und Weise ist eine individuelle Verschlüsselung einzelner Betriebsphasen (beispielsweise einzelner? Fahrten) des Kraftfahrzeugs möglich. Dies ermöglicht einen besonders sicheren Betrieb des beschriebenen Verfahrens. Insbesondere ist es möglich, dass Fahrzeugführer die geheimen Schlüssel ihres jeweiligen zweiten Schlüsselpaars nicht anderen Fahrzeugführern zur Verfügung stellen müssen.

[0034] Das Verfahren ist besonders vorteilhaft, wenn die Bereitstellung des zweiten öffentlichen Schlüssels des zweiten Schlüsselpaars über eine Schlüsselaustausch-Schnittstelle erfolgt.

[0035] Die Schlüsselaustauschschnittstelle kann beispielsweise eine WLAN-Schnittstelle, eine Bluetooth-Schnittstelle oder eine andere kontaktlose Schnittstelle sein. Solche Schnittstellen sind bei üblichen mobilen Endgeräten grundsätzlich verfügbar und auch übliche Kraftfahrzeuge verfügen über solche Schnittstellen. Über solche Schnittstellen kann die Bereitstellung des zweiten öffentlichen Schlüssels für das Verfahren und für den Betriebsdatenrekorder einfach erfolgen. Insbesondere, wenn das separate elektronische Gerät ein Mobiltelefon des Fahrzeugführers des Kraftfahrzeuges ist und das Kraftfahrzeug beispielsweise eine Freisprecheinrichtung aufweist, erfolgt üblicherweise ein Verbinden des separaten elektronischen Gerätes und des Kraftfahrzeuges bei Inbetriebnahme des Kraftfahrzeuges bzw. der Freisprecheinrichtung.

[0036] Das Verfahren ist besonders vorteilhaft, wenn die Bereitstellung des zweiten öffentlichen Schlüssels des zweiten Schlüsselpaars einen Fingerabdruckabgleich eines Fingerabdrucks des zweiten Schlüsselpaars umfasst.

[0037] Der Fingerabdruckabgleich kann dazu dienen, zu erkennen, ob in dem Betriebsdatenrekorder für die Durchführung des beschriebenen Verfahrens tatsächlich der gewünschte, üblicherweise gerade bereitgestellte zweite öffentliche Schlüssel des Fahrzeugführers angelangt ist. Über den Fingerabdruck kann ein falscher Schlüssel sehr schnell identifiziert werden. Als Fingerabdruck kann beispielsweise ein aus dem zweiten öffentlichen Schlüssel generierter Hashwert verwendet werden. Der Fingerabdruckabgleich kann beispielsweise auch teilautomatisch oder ganz automatisch erfolgen, so dass der Fahrzeugführer keine manuelle Aktion mehr durchführen muss, um den Fingerabdruckabgleich durchzuführen. Eine Möglichkeit zum teilautomatisierten Fingerabdruckabgleich ist, dass bei einem Display in dem Kraftfahrzeug ein QR-Code angezeigt wird, auf welchem eine Kamera eines mobilen Endgerätes gerichtet wird. In dem QR-Code kann der Hashwert bzw. der Fingerabdruck des Schlüssels enthalten sein. Durch die Kamera des Mobiltelefons wird der Hashwert bzw. der Fingerabdruck übertragen. So kann das mobile Endgerät bzw. das separate elektronische Gerät erkennen, ob der jeweils richtige zweite öffentliche Schlüssel verwendet wird.

[0038] Hier auch beschrieben werden soll ein Betriebsdatenrekorder für ein Kraftfahrzeug, der zur

Durchführung des beschriebenen Verfahrens eingerichtet ist.

[0039] Außerdem beschrieben werden soll ein Computerprogrammprodukt, eingerichtet zur Durchführung des beschriebenen Verfahrens.

[0040] Darüber hinaus beschrieben werden soll ein maschinenlesbares Speichermedium, auf dem ein solches Computerprogrammprodukt gespeichert ist.

[0041] Das hier beschriebene Verfahren wird nachfolgend anhand der Figuren näher erläutert.

[0042] Es zeigen:

Fig. 1: ein Kraftfahrzeug eingerichtet zur Durchführung des beschriebenen Verfahrens,

Fig. 2: einen Entschlüsselungsvorgang zur Entschlüsselung von mit dem beschriebenen Verfahren verschlüsselten Betriebsdaten.

[0043] **Fig. 1** zeigt ein Kraftfahrzeug **1** mit einem Betriebsdatenrekorder **6**. Der Betriebsdatenrekorder **6** hat eine Datenschnittstelle **16** über welche Sensordaten von Sensoren **5** als Betriebsdaten dem Betriebsdatenrekorder **6** zur Verfügung gestellt werden. In dem Betriebsdatenrekorder **6** ist ein volatiler Speicher **9** sowie ein nicht volatiler Speicher **8** vorgesehen. Diese Aufteilung auf einen volatilen Speicher **9** und einen nicht volatilen Speicher **8** ist nicht zwangsläufig und kann im Bedarfsfall auch anders gewählt werden.

[0044] Ein erster öffentlicher Schlüssel **2a** wird aus dem nicht volatilen Speicher **8** entnommen. Dies entspricht Schritt **a)** des beschriebenen Verfahrens, ein zweiter öffentlicher Schlüssel **3a** wird von einem separaten elektronischen Gerät **7** bereitgestellt. Dies geschieht über eine Schlüsselaustauschschnittstelle **10**, wobei bevorzugt auch ein Fingerabdruckabgleich **11** erfolgt, um die Echtheit des zweiten öffentlichen Schlüssels **3a** zu verifizieren. Dies entspricht Schritt **b)** des beschriebenen Verfahrens.

[0045] Die über die Datenschnittstelle **16** gewonnenen Daten stehen als Betriebsdaten **13** zur Verfügung. Das Einsammeln dieser Daten entspricht Schritt **c)** des beschriebenen Verfahrens. In dem Betriebsdatenrekorder **6** erfolgt nun die Verschlüsselung der Daten. Im hier vorliegenden Beispiel erfolgt zunächst ein zweiter Verschlüsselungsprozess **3d**, sodass einfach verschlüsselte Daten **14** entstehen. Anschließend erfolgt ein erster Verschlüsselungsprozess **2d**, so dass doppelt verschlüsselte Betriebsdaten **15** entstehen. Diese doppelt verschlüsselten Betriebsdaten **15** werden dann bereitgestellt (Schritt **e)**. Die Bereitstellung dieser Daten umfasst ein Ablegen der Daten in dem nicht volatilen Speicher **8**. Es sind andere Ablagemöglichkeiten der verschlüsselten Betriebsdaten **15** möglich, wie weiter vorne ausgeführt wurde. Beispielsweise eine Ablage der verschlüsselten Betriebsdaten **15** auch in dem separaten elektronischen Gerät **7**. Die Durchführung der Verschlüsselungsvorgänge entspricht Schritt **d)** des beschriebenen Verfahrens.

[0046] **Fig. 2** zeigt wie die mit dem beschriebenen Verfahren gewonnenen Daten wieder entschlüsselt werden können. Hier zu erkennen sind schematisch der Betriebsdatenrekorder **6** sowie der nicht volatile Speicher **8** in welchem die doppelt verschlüsselten Daten **15** vorliegen. Die Entschlüsselung erfolgt bevorzugt in einer Entschlüsselungssphäre **12**, die insbesondere dadurch gekennzeichnet ist, dass ihr die Inhaber beider geheimer Schlüssel, also sowohl die für den Betrieb des Kraftfahrzeugs verantwortliche Stelle als auch der Fahrzeugführer des Kraftfahrzeuges, vertrauen können. Dies kann beispielsweise in einem Verfahren zur Klärung des Ablaufs eines Unfalls sein. Hier erfolgt die Entschlüsselung mit dem ersten Geheimschlüssel **2b** mit einem ersten Entschlüsselungsprozesss **2e** und mit dem zweiten Geheimschlüssel **3b** mit einem zweiten Entschlüsselungsprozess **3e** in zur erfolgten Verschlüsselung umgekehrten Reihenfolge, so dass zunächst einfach verschlüsselte Daten **14** entstehen und anschließend wieder die Betriebsdaten **13** als Rohdaten entstehen.

Patentansprüche

1. Verfahren zur Speicherung von Betriebsdaten, die während eines Betriebs des Kraftfahrzeuges (1) mit einem Fahrzeugführer entstehen, wobei die Betriebsdaten bei der Speicherung derart verschlüsselt werden, dass zum Entschlüsseln der Betriebsdaten eine Mitwirkung des Fahrzeugführers des Kraftfahrzeugs (1) erforderlich ist.

2. Verfahren nach Anspruch 1, aufweisend die folgenden Schritte:
a) Ermitteln eines ersten öffentlichen Schlüssels (2a) eines ersten Schlüsselpaars, dessen erster geheimer Schlüssel (2b) in einer ersten geschützten Sphäre (2c) einer für den technischen Betrieb des Kraftfahrzeugs (1) verantwortlichen Stelle ist,
b) Ermitteln eines zweiten öffentlichen Schlüssels (3a) eines zweiten Schlüsselpaars, dessen geheimer Schlüssel (3b) in einer zweiten geschützten Sphäre (3c) eines Fahrzeugführers des Kraftfahrzeugs (1) ist,
c) Akquirieren von Betriebsdaten des Kraftfahrzeuges (1) während eines Betriebs des Kraftfahrzeuges (1),
d) Verschlüsseln der Betriebsdaten mit dem ersten öffentlichen Schlüssel (2a) und dem zweiten öffentlichen Schlüssel (3a), und
e) Ablegen der verschlüsselten Betriebsdaten auf einem Datenspeicher (4).

3. Verfahren nach Anspruch 2, wobei Betriebsdaten zumindest eine der folgenden Arten von Daten umfassen:
- Sensordaten von Sensoren (5) zur Überwachung des Umfeldes des Kraftfahrzeugs (1),
- Sensordaten von Sensoren (5) zur Überwachung des Innenraums des Kraftfahrzeugs (1),
- Messdaten, zur Überwachung von Insassen des Kraftfahrzeugs (1), und
- Kameraaufnahmen.

4. Verfahren nach Anspruch 2 oder 3, wobei das Verfahren in einem Betriebsdatenrekorder (6) des Kraftfahrzeuges (1) durchgeführt wird.

5. Verfahren nach Anspruch 4, wobei der Datenspeicher (4) in dem Betriebsdatenrekorder (6) des Kraftfahrzeugs (1) angeordnet ist.

6. Verfahren nach Anspruch 5, wobei der Datenspeicher (4) in einem von dem Kraftfahrzeug (1) separaten elektronischen Gerät (7) angeordnet ist.

7. Verfahren nach Anspruch 6, wobei das elektronische Gerät (7) ein mobiles Endgerät des Fahrzeugführers des Kraftfahrzeugs (1) ist.

8. Verfahren nach einem der vorhergehenden Ansprüche, wobei der erste öffentliche Schlüssel (2a) des ersten Schlüsselpaars in Schritt a) aus einem nicht volatilen Speicher (8) in dem Kraftfahrzeug (1) ermittelt wird.

9. Verfahren nach einem der vorhergehenden Ansprüche, wobei der zweite öffentliche Schlüssel (3a) des zweiten Schlüsselpaars in Schritt b) von einem separaten elektronischen Gerät (7) bereitgestellt wird.

10. Verfahren nach Anspruch 9, wobei der zweite öffentliche Schlüssel (3a) des zweiten Schlüsselpaars vor dem Start einer Betriebsphase des Kraftfahrzeugs (1) in dem von dem Kraftfahrzeug (1) separaten elektronischen Gerät (7) generiert wird.

11. Verfahren nach Anspruch 9 oder 10, wobei die Bereitstellung des zweiten öffentlichen Schlüssels (3a) des zweiten Schlüsselpaars über eine Schlüsselaustauschschnittstelle (10) erfolgt.

12. Verfahren nach einem der Ansprüche 9 bis 11, wobei die Bereitstellung des zweiten öffentlichen Schlüssels (3a) des zweiten Schlüsselpaars einen Fingerabdruckabgleich (11) eines Fingerabdrucks des zweiten Schlüsselpaars umfasst.

13. Betriebsdatenrekorder (6) für ein Kraftfahrzeug (1), der zur Durchführung des Verfahrens nach einem der Ansprüche 1 bis 12 eingerichtet ist.

14. Computerprogrammprodukt eingerichtet zur Durchführung des Verfahrens nach einem der Ansprüche 1 bis 12.

15. Maschinenlesbares Speichermedium auf dem ein Computerprogrammprodukt nach Anspruch 13 gespeichert ist.

Es folgt eine Seite Zeichnungen

Anhängende Zeichnungen

Fig. 1

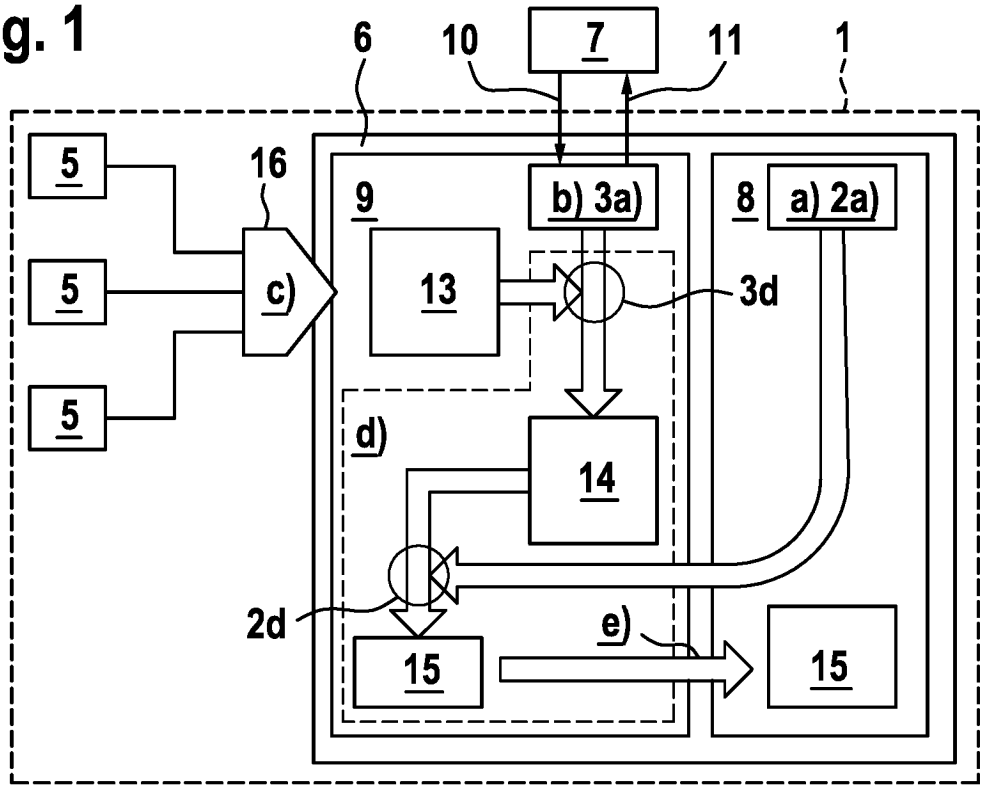


Fig. 2