(19) österreichisches patentamt

(10) **AT 520029 B1 2019-04-15**

(12) **Patentschrift**

(21) Anmeldenummer: A 50384/2017
(22) Anmeldetag: 10.05.2017
(45) Veröffentlicht am: 15.04.2019

(51) Int. Cl.: ***G06F 12/14*** (2006.01)
G06F 21/60 (2013.01)
G06F 21/72 (2013.01)

(56) Entgegenhaltungen:
CN 104461946 A
US 2014365725 A1
US 2010177901 A1
CN 105825136 A
US 8819383 B1

(73) Patentinhaber:
Pronextor GmbH
2333 Leopoldsdorf bei Wien (AT)

(72) Erfinder:
Kollmitzer Christian Dipl.Ing.
9061 Klagenfurt-Wölfnitz (AT)

(74) Vertreter:
Wildhack & Jellinek Patentanwälte OG
1030 Wien (AT)

(54) **Zugriffssteuerungseinheit zur Steuerung des Zugriffs auf in einem Datenspeicher gespeicherte verschlüsselte Daten**

(57) Die Erfindung betrifft eine Zugriffssteuerungseinheit (1) zur Steuerung des Zugriffs auf in einem Datenspeicher (2) gespeicherte verschlüsselte Daten (DV), umfassend eine erste physikalische Schnittstelle (11) zum Anschluss an zumindest einen Datenspeicher (2), eine zweite physikalische Schnittstelle (12) zum Anschluss an einen Rechner (3), eine Schlüsseleingabeeinheit (13) und einen Prozessor (14)

- wobei die erste physikalische Schnittstelle (11) zum Zugriff auf zumindest einen auf zumindest einem Datenspeicher (2) abgespeicherten Container (C) ausgebildet ist,
- wobei die Zugriffssteuerungseinheit (1) dazu ausgebildet ist, über die zweite physikalische Schnittstelle (12) nach einem vorgegebenen Protokoll Zugriff auf ein virtuelles Laufwerk zu gewähren,
- wobei die Schlüsseleingabeeinheit (13) zur Eingabe eines Schlüssels (S) durch einen Benutzer ausgebildet ist,
- wobei der Prozessor (14) dazu ausgebildet ist, bei Vorliegen einer Leseanfrage (L) an der zweiten physikalischen Schnittstelle (12) eine diesbezügliche Zugriffsanfrage an der ersten physikalischen Schnittstelle (11) bereitzustellen und über die zweite physikalische Schnittstelle (12) auf die in zumindest einem Container (C) auf dem zumindest einen Datenspeicher (2) gespeicherten Daten (DV) zuzugreifen und den Inhalt des Containers (C) mit dem Schlüssel (S) zu entschlüsseln und an der zweiten physikalischen Schnittstelle (12) bereitzustellen.

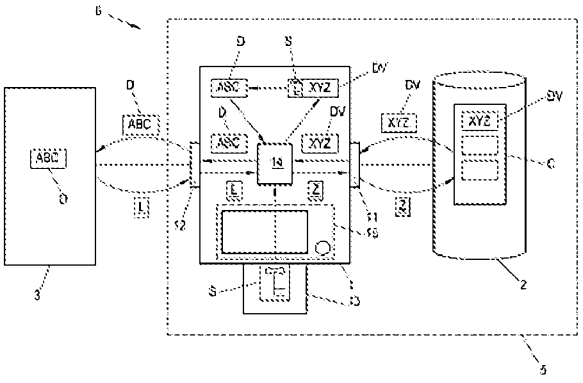

Fig. 1

AT 520029 B1 2019-04-15

Beschreibung

[0001] Die Erfindung betrifft eine Vorrichtung gemäß dem Oberbegriff des Patentanspruchs 1 sowie ein Verfahren gemäß dem Patentanspruch 9.

[0002] Aus dem Stand der Technik sind Verfahren zur Verschlüsselung von Daten in einem Datenspeicher bekannt. Derartige Verfahren erstellen beispielsweise virtuelle Laufwerke, die mit einem ausgewählten Schlüssel verschlüsselt werden und nur nach Eingabe eines zugeteilten Schlüssels zugänglich sind. Auf diese Weise lassen sich einzelne Verzeichnisse, externe Speichermedien oder Festplatten sichern.

[0003] Nachteil bei derartigen Verfahren ist allerdings, dass der zum Entschlüsseln benötigte Schlüssel ständig im Arbeitsspeicher des Rechners, der auf das verschlüsselte Laufwerk zugreift, gespeichert sein muss, um einen dauerhaften Zugriff auf die betreffenden Daten zu gewährleisten. Durch Schadsoftware oder hardwareseitig Kompromittierung des Systems kann der benötigte Schlüssel ermittelt werden, sodass ein unerwünschter Zugriff und eine Entschlüsselung der gespeicherten Daten erfolgen können.

[0004] Durch das Speichern des Schlüssels im Arbeitsspeicher des Rechners ergibt sich ein weiterer Nachteil bekannter Verfahren: Wenn der Rechner in den Hibernation-Modus, also den Ruhezustand, wechselt, wird der Inhalt des Arbeitsspeichers auf die Festplatte geschrieben und alle Systemkomponenten werden ausgeschaltet, damit bei Einschalten des Rechners das auf der Festplatte gespeicherte Abbild wieder in den Arbeitsspeicher geladen werden kann. Wenn ein tragbarer Rechner beispielsweise entwendet wird, und durch Schließen in den Hibernation-Modus gebracht wird, kann dadurch der Zugriff auf gespeicherte Daten erfolgen.

[0005] Aufgabe der vorliegenden Erfindung ist es, eine Vorrichtung und ein Verfahren der eingangs genannten Art zu schaffen, die eine zuverlässige Steuerung des Zugriffs auf verschlüsselte Daten in einem Datenspeicher zu ermöglichen.

[0006] Diese Ziele werden mit den kennzeichnenden Merkmalen des Anspruchs 1 erreicht. Erfindungsgemäß ist vorgesehen, dass
- die erste physikalische Schnittstelle zum Zugriff auf zumindest einen auf zumindest einem Datenspeicher abgespeicherten Container ausgebildet ist,
- wobei die Zugriffssteuerungseinheit dazu ausgebildet ist, über die zweite physikalische Schnittstelle nach einem vorgegebenen Protokoll Zugriff auf ein virtuelles Laufwerk zu gewähren,
- wobei die Schlüsseleingabeeinheit zur Eingabe eines Schlüssels durch einen Benutzer ausgebildet ist,
- wobei der Prozessor dazu ausgebildet ist, bei Vorliegen einer Leseanfrage an der zweiten physikalischen Schnittstelle eine diesbezügliche Zugriffsanfrage an der ersten physikalischen Schnittstelle bereitzustellen und über die zweite physikalische Schnittstelle auf die in zumindest einem Container auf dem zumindest einen Datenspeicher gespeicherten Daten zuzugreifen und den Inhalt des Containers mit dem Schlüssel zu entschlüsseln und an der zweiten physikalischen Schnittstelle bereitzustellen.

[0007] Von Vorteil ist dabei die hardwaremäßige Trennung des Schlüssels von den gespeicherten Daten. Insbesondere kann ein Angriff auf ein mittels der erfindungsgemäßen Vorrichtung erstelltes System nur dann erfolgreich sein, wenn sowohl das System als auch die Vorrichtung unter Kontrolle des Angreifers ist.

[0008] Zum sicheren Speichern von Daten auf einem Datenspeicher ist vorteilhafterweise vorgesehen, dass der Prozessor dazu ausgebildet ist, bei Vorliegen eines Schreibanfrage die zu schreibenden Daten zu verschlüsseln und im Container auf dem Datenspeicher abzuspeichern.

[0009] Um ein unerwünschtes Übertragen großer Datenmengen zu erkennen und zu unterbrechen, ist vorgesehen, dass der Prozessor zur Überwachung des Datenverkehrs über die zweite Schnittstelle und zur Erstellung eines Alarmhinweises ausgebildet ist, wenn die Datenübertragungsrate oder die Rate der pro Zeiteinheit übertragenen Dateien einen vorgegebenen ersten

Grenzwert überschreitet, und
- dass die Zugriffssteuerungseinheit eine Anzeigeeinheit zur Anzeige eines solchen Alarmhinweises umfasst und der Prozessor dazu ausgebildet ist, in diesem Fall dem Benutzer die Möglichkeit zum manuellen Unterbrechung der Datenübertragung zu ermöglichen, und/oder
- dass der Prozessor dazu ausgebildet ist, bei Überschreiten eines den ersten Grenzwert übersteigenden vorgegebenen zweiten Grenzwerts die Datenübertragung zu unterbrechen.

[0010] Vorteilhafterweise ist auch vorgesehen, dass die erste physikalische Schnittstelle zum Zugriff auf mehrere auf einem Datenspeicher abgespeicherten Container ausgebildet ist, wobei die in den jeweiligen Containern gespeicherten Daten vorzugsweise mit verschiedenen Schlüsseln verschlüsselt sind und die Schlüsseleingabeeinheit die Eingabe mehrerer Schlüssel ermöglicht und wobei der Prozessor die Zuordnung der Schlüssel zu den zugehörigen verschlüsselten Daten ermöglicht.

[0011] Die Möglichkeit, auch mehrere Datenspeicher gleichzeitig an die Zugriffssteuerungseinheit anschließen zu können, ist vorteilhafterweise gegeben dadurch, dass zumindest eine weitere physikalische Schnittstelle zum Anschluss an zumindest einen weiteren Datenspeicher sowie zum Zugriff auf zumindest einen weiteren Container auf dem Datenspeicher vorgesehen ist.

[0012] Eine höhere Ausfallsicherheit wird vorteilhafterweise erzielt, indem die erste physikalische Schnittstelle zum Zugriff auf einen auf mehrere Datenspeicher verteilt gespeicherten Container ausgebildet ist, wobei der Prozessor dazu ausgebildet ist, entsprechend der für die verteilte Speicherung vorgegebenen logische Zuordnung
bei Vorliegen einer Leseanfrage einzelne denselben Container betreffende Datenspeicher auszulesen und die so erhaltenen Speicherwerte aufgrund des Schlüssels zu entschlüsseln und an die zweite Schnittstelle weiterzuleiten, und
insbesondere bei Vorliegen einer Schreibanfrage die zu schreibenden Daten mit dem Schlüssel zu verschlüsseln und die derart ermittelten Verschlüsselungsergebnisse auf einzelne denselben Container betreffende Datenspeicher zu schreiben.

[0013] Dass der zum Verschlüsseln und Entschlüsseln der Daten notwenige Schlüssel nicht im Arbeitsspeicher des Rechners, der auf das verschlüsselte Laufwerk zugreift, gespeichert sein muss, wird erzielt, indem die Schlüsseleingabeeinheit zur Eingabe oder Erfassung eines Schlüssels S zumindest einer der folgenden Arten ausgebildet ist:
- Einlesen des den Schlüssel enthaltenden zweidimensionalen Codes, insbesondere Barcodes oder QR-Codes, mittels einer optischen Leseeinheit,
- Einlesen eines Schlüssels von einem Datenträger, z. B. von einem USB-Stick,
- Einlesen des Schlüssels von einem NFC-fähigen Hardware-Item mittels NFC,
- Manuelle Eingabe des Schlüssels durch einen Benutzer.

[0014] Sicheres Speichern von verschlüsselten Daten in einem Datenspeicher wird gewährleistet durch eine Speichereinheit umfassend eine Zugriffssteuerungseinheit nach einem der vorangehenden Ansprüche sowie zumindest einen Datenspeicher, wobei der Datenspeicher über die erste physikalische Schnittstelle an die Zugriffssteuerungseinheit angeschlossen ist.

[0015] Sicheres Zugreifen auf verschlüsselten Daten in einem Datenspeicher wird gewährleistet durch ein System umfassend eine Speichereinheit nach Anspruch 8 sowie einen Rechner, wobei der Rechner über die zweite physikalische Schnittstelle an die Zugriffssteuerungseinheit angeschlossen ist.

[0016] Zum sicheren Zugriff auf verschlüsselte Daten in einem Datenspeicher ist vorgesehen,
- dass die Zugriffssteuerungseinheit einen durch einen Benutzer eingegebenen Schlüssel ermittelt,
- wobei der Rechner eine Leseanfrage über die zweite physikalische Schnittstelle an die Zugriffssteuerungseinheit übermittelt,
- wobei die Zugriffssteuerungseinheit nach einem vorgegebenen Protokoll die Leseanfrage an den Datenspeicher weiterleitet,
- wobei der Datenspeicher die der Leseanfrage entsprechenden verschlüsselten Daten an die

Zugriffssteuerungseinheit übermittelt,
- wobei die Zugriffssteuerungseinheit die vom Datenspeicher übermittelten verschlüsselten Daten mit dem Schlüssel entschlüsselt,
- wobei die Zugriffssteuerungseinheit die entschlüsselten Daten über die zweite physikalische Schnittstelle an den Rechner übermittelt.

[0017] Zum sicheren Speichern von Daten in einem Datenspeicher ist vorgesehen, dass der Rechner eine Schreibanfrage und auf den Datenspeicher zu speichernde Daten über die zweite physikalische Schnittstelle an die Zugriffssteuerungseinheit übermittelt,
- wobei die Zugriffssteuerungseinheit die vom Rechner übermittelten Daten mit dem Schlüssel verschlüsselt,
- wobei die Zugriffssteuerungseinheit nach einem vorgegebenen Protokoll die verschlüsselten Daten und die Schreibanfrage über die erste physikalische Schnittstelle an den Datenspeicher übermittelt.
- wobei die verschlüsselten Daten in einem Container auf dem Datenspeicher gespeichert werden.

[0018] Zum verbesserten Schutz vor unerwünschten Zugriffen auf Daten in einem Datenspeicher ist vorgesehen, dass die Zugriffssteuerungseinheit der Datenverkehr über die zweite Schnittstelle überwacht,
- wobei bei Überschreiten eines vorgegebenen ersten Grenzwerts der Datenübertragungsrate ein Alarmhinweis von der Zugriffssteuerungseinheit erzeugt und angezeigt wird dem Benutzer die Möglichkeit zur Unterbrechung des Datenverkehrs über die erste Schnittstelle geboten wird und/oder
- wobei die Datenübertragung über die zweite Schnittstelle bei Überschreiten eines vorgegebenen den ersten Grenzwert überschreitenden zweiten Grenzwerts die, insbesondere ohne erforderliche Benutzerinteraktion, unterbrochen wird.

[0019] Um einen unerwünschten Zugriff auf Daten in einem Datenspeicher effektiv zu verhindern, ist vorgesehen, dass der erste und/oder zweite Grenzwert der Datenübertragungsrate vorgegeben wird als eine maximale Datenmenge pro Zeiteinheit und/oder eine Anzahl von Dateien pro Zeiteinheit, wobei insbesondere
- der erste und/oder zweite Grenzwert abhängig von einer Uhrzeit vorgegeben wird.

[0020] Um eine höhere Ausfallsicherheit und einen größeren Datendurchsatz durch Verwendung mehrerer Datenspeicher ausnutzen zu können, ist vorteilhafterweise vorgesehen, dass die Zugriffssteuerungseinheit auf einen auf mehrere Datenspeicher verteilten Container zugreift.

[0021] Weiters ist vorteilhafterweise vorgesehen, dass der Schlüssel entsprechend vorgegebener Kriterien permanent gehalten wird, insbesondere für eine Anzahl von Zugriffen und/oder eine Zeitspanne.

[0022] Die Erfindung ist im Folgenden anhand von besonders vorteilhaften, aber nicht einschränkend zu verstehenden, Ausführungsbeispielen in den Zeichnungen schematisch dargestellt und wird unter Bezugnahme auf die Zeichnungen beispielhaft beschrieben:

[0023] Fig. 1 zeigt eine bevorzugte Ausführungsform einer erfindungsgemäßen Zugriffssteuerungseinheit sowie das Vorgehen beim Auslesen von verschlüsselten Daten gemäß einer bevorzugten Variante der Erfindung.

[0024] Fig. 2 das Schreiben von verschlüsselten Daten gemäß einer bevorzugten Variante der Erfindung bei der in Fig. 1 dargestellten Zugriffssteuerungseinheit.

[0025] Fig. 3 zeigt eine Speichereinheit mit einer erfindungsgemäßen Zugriffssteuerungseinheit.

[0026] Fig. 4 zeigt eine bevorzugte Ausführungsform einer erfindungsgemäßen Zugriffssteuerungseinheit mit einer Vielzahl von angeschlossenen Speichereinheiten.

[0027] In Fig. 1 sind eine mögliche Ausführungsform einer erfindungsgemäßen Zugriffssteuerungseinheit 1 und der Ablauf einer Variante eines erfindungsgemäßen Verfahrens zum Zugriff

eines Rechners 3 auf in einem Datenspeicher 2 gespeicherte verschlüsselte Daten DV mittels der Zugriffssteuerungseinheit 1 schematisch dargestellt.

[0028] Fig. 1 zeigt ein System 6 umfassend eine Speichereinheit 5, welche eine Zugriffssteuerungseinheit 1 und einen Datenspeicher 2 beinhaltet, und einen Rechner 3, wobei auf dem Datenspeicher 2 in einem Container C verschlüsselte Daten DV gespeichert sind.

[0029] Die Zugriffssteuerungseinheit 1 umfasst im gezeigten Ausführungsbeispiel eine erste physikalische Schnittstelle 11, eine zweite physikalischen Schnittstelle 12, eine Schlüsseleingabeeinheit 13, einen Prozessor 14 und eine Anzeigeeinheit 15. Die Anzeigeeinheit 15 umfasst im Ausführungsbeispiel eine LED und ein Display.

[0030] Der Datenspeicher 2 ist über die erste physikalische Schnittstelle 11 an die Zugriffssteuerungseinheit 1 angeschlossen. Der Rechner 3 ist über die zweite physikalische Schnittstelle 12 an die Zugriffssteuerungseinheit 1 angeschlossen. Die Datenverbindung der Zugriffssteuerungseinheit 1 mit dem Rechner 3 oder dem Datenspeicher 2 kann beispielsweise per Kabel, insbesondere über ein USB-Kabel hergestellt werden. Bei der Erfindung ist auch eine Datenverbindung per Funk technisch möglich, wobei jedoch eine Verbindung per Kabel regelmäßig einen höheren Schutz vor unerwünschten Zugriffen bietet.

[0031] Die Zugriffssteuerungseinheit 1 gewährt einem über die zweite physikalische Schnittstelle 12 an die Zugriffssteuerungseinheit 1 angeschlossenen Rechner 3 nach einem vorgegebenen Protokoll Zugriff auf ein von der Zugriffssteuerungseinheit 1 verwaltetes virtuelles Laufwerk. Als Protokoll für den Datenaustausch zwischen der Zugriffssteuerungseinheit 1 und dem Rechner 3 kann dabei beispielsweise das für USB- Datenträger verwendete Protokoll verwendet werden.

[0032] Bei Eingabe eines Schlüssels S über die Schlüsseleingabeeinheit 13 durch einen Benutzer ermittelt der Prozessor 14 der Zugriffssteuerungseinheit 1 den Schlüssel S ermittelt. Der Schlüssel S wird dabei für eine definierte Anzahl an Lese- und Schreibanfragen basierend auf konfigurierbaren Parametern wie beispielsweise der Zeitspanne oder der Anzahl an Zugriffen permanent gehalten. Der Schlüssel S kann durch diesbezügliche Betätigung der Schlüsseleingabeeinheit 13 entfernt werden.

[0033] Weiters kann auch vorgesehen sein, dass über die Anzeigeeinheit 15 ein konkreter Container C auf dem Datenträger 2 ausgewählt werden kann, auf den mittels des Schlüssels S zugegriffen werden soll.

[0034] Bei Vorliegen einer vom Rechner 3 an die Zugriffssteuerungseinheit 1 übermittelten Leseanfrage L an der zweiten physikalischen Schnittstelle 12, stellt der Prozessor 14 der Zugriffssteuerungseinheit 1 nach einem vorgegebenen Protokoll eine diesbezügliche Zugriffsanfrage Z an der ersten physikalischen Schnittstelle 11 bereit. Die Zugriffsanfrage Z wird über die erste physikalische Schnittstelle 11 an den Datenspeicher 2 übermittelt, wodurch der Prozessor 14 auf die in einem Container C auf dem Datenspeicher 2 gespeicherten Daten DV zugreifen und die der Zugriffsanfrage Z entsprechenden verschlüsselten Daten DV im Container C ermitteln kann.

[0035] Bei einigen Verschlüsselungsverfahren ist es auch erforderlich, dass zum Auslesen des Speichers an einer bestimmten Speicherstelle entsprechend dem verwendeten Schlüssel unterschiedliche Speicherpositionen innerhalb des Containers C ausgelesen werden müssen. In diesem Fall ermittelt der Prozessor 14 eine oder mehrere Speicherpositionen innerhalb des Containers C, die für die Bestimmung des Werts der vom Rechner abgefragten, insbesondere virtuellen, Speicherposition erforderlich sind.

[0036] Die ermittelten verschlüsselten Daten DV werden an der ersten physikalischen Schnittstelle 11 bereitgestellt und vom Prozessor 14 mithilfe des ermittelten Schlüssels S entschlüsselt. Anschließend werden die entschlüsselten Daten D vom Prozessor 14 an der zweiten physikalischen Schnittstelle 12 der Zugriffssteuerungseinheit 1 nach einem vorgegebenen Protokoll bereitgestellt, von wo aus die entschlüsselten Daten D an den Rechner 2 übermittelt werden.

Der Schlüssel S wird dabei für eine definierte Anzahl an Lesezugriffen basierend auf konfigurierbaren Parametern wie beispielsweise der Zeitspanne oder der Anzahl an Zugriffen permanent gehalten.

[0037] Ein derartiges Verfahren verhindert zuverlässig ein unerwünschtes Auslesen der verschlüsselten Daten DV, da der zum Entschlüsseln der verschlüsselten Daten DV benötigte Schlüssel S nicht im Rechner 3 gespeichert ist, sondern physikalisch vom Rechner 3 getrennt über die Schlüsseleingabeeinheit 14 der Zugriffssteuerungseinheit 1 eingegeben wird. Sofern die Zugriffssteuerungseinheit 1 nicht ihrerseits korrumpiert ist, erhält der Rechner 3 weder Zugriff auf den Schlüssel, noch auf die auf dem Datenträger 2 abgespeicherten verschlüsselten Daten.

[0038] Wird ein falscher Schlüssel S eingegeben, stellt der Prozessor 14 der Zugriffssteuerungseinheit 1 zwar bei Vorliegen einer Leseanfrage L vom Rechner 3 an der zweiten physikalischen Schnittstelle 12 eine diesbezügliche Zugriffsanfrage Z an der ersten physikalischen Schnittstelle 11 bereit, wodurch die Zugriffsanfrage Z an den Datenspeicher 2 übermittelt wird und die der Zugriffsanfrage Z entsprechenden verschlüsselten Daten DV an der ersten physikalischen Schnittstelle 11 bereitgestellt werden. Da der Schlüssel jedoch nicht korrekt ist und nicht dem für die Entschlüsselung erforderlichen Schlüssel entspricht, werden vom Prozessor 14 Daten an der zweiten physikalischen Schnittstelle 12 bereitgestellt und an den Rechner 3 übermittelt, die idR nicht einmal das Mounten bzw. Einhängen eines virtuellen Laufwerks erlauben. Es kommen am Rechner 3 bedeutungslose Daten an, deren Bedeutung ohne den entsprechenden Schlüssel S nicht erfassbar ist, wodurch ein unerwünschtes Auslesen zuverlässig verhindert wird.

[0039] In Fig. 2 ist schematisch das Speichern von Daten gemäß einer vorteilhaften Ausführungsform der Erfindung dargestellt. Bei Vorliegen einer vom Rechner 3 an die Zugriffssteuerungseinheit 1 übermittelten Schreibanfrage W umfassend die unverschlüsselten zu speichernden Daten D sowie die betreffende Speicherposition an der zweiten physikalischen Schnittstelle 12, verschlüsselt der Prozessor 14 der Zugriffssteuerungseinheit 1 die unverschlüsselten zu speichernden Daten D mit dem ermittelten Schlüssel S und stellt die verschlüsselten Daten DV gemeinsam mit einer nach einem vorgegebenen Protokoll erstellten diesbezüglichen Schreibanfrage Z' an der ersten physikalischen Schnittstelle 11 bereit.

[0040] Sofern es nach dem betreffenden Verschlüsselungsprotokoll erforderlich ist, können dem Abspeichern der verschlüsselten Daten auch noch Leseschritte auf dem Datenträger vorangehen. Ebenso kann es durch das betreffende Protokoll vorgegeben sein, dass vor dem Abspeichern noch die einzelnen Positionen ermittelt werden, an denen die verschlüsselten Daten abgespeichert werden.

[0041] Die verschlüsselten Daten DV und die Schreibanfrage Z' werden über die erste physikalische Schnittstelle 11 an den Datenspeicher 2 übermittelt und die verschlüsselten Daten DV werden entsprechend der Schreibanfrage Z' in einem Container C auf dem Datenspeicher 2 gespeichert.

[0042] In Fig. 3 ist eine Speichereinheit 5 dargestellt, die eine Zugriffssteuerungseinheit 1 und einen Datenspeicher 2 umfasst, sowie weiters ein Rechner 3 zum Verarbeiten der von der Speichereinheit 5 zur Verfügung gestellten Daten.

[0043] Die Zugriffssteuerungseinheit 1 umfasst im dargestellten Ausführungsbeispiel eine erste physikalischen Schnittstelle 11, eine zweite physikalische Schnittstelle 12, eine Schlüsseleingabeeinheit 13 einen Prozessor 14 und eine Anzeigeeinheit 15 mit einer LED und einem Display. Der Datenspeicher 2 ist über die erste physikalische Schnittstelle 11 an die Zugriffssteuerungseinheit 1 angeschlossen und der Rechner 3 ist über die zweite physikalische Schnittstelle 12 an die Zugriffssteuerungseinheit 1 angeschlossen. Die Zugriffssteuerungseinheit 1 gewährt einem über die zweite physikalische Schnittstelle 12 an die Zugriffssteuerungseinheit 1 angeschlossenen Rechner 2 nach einem vorgegebenen Protokoll Zugriff auf ein virtuelles Laufwerk.

[0044] Bei allen voranstehend beschriebenen Varianten eines erfindungsgemäßen Verfahrens

bzw. allen Ausführungsformen einer Zugriffssteuerungseinheit 1 kann vorteilhafterweise vorgesehen sein, dass der Prozessor 14 den Datenverkehr zwischen Rechner 3 und Zugriffssteuerungseinheit 1 überwacht wird und bei Überschreiten eines vorgegebenen Grenzwerts der Datenübertragungsrate einen Alarmhinweis erzeugt, da eine hohe Datenübertragungsrate auf ein möglicherweise unerwünschtes Übertragen großer Datenmengen hindeutet. Dies kann beispielsweise durch Aktivierung einer LED erfolgen. Der Alarmhinweis wird von der Zugriffssteuerungseinheit 1 angezeigt, alternativ kann diese auch über einen Lautsprecher ein akustisches Warnsignal abgeben.

[0045] Die Zugriffssteuerungseinheit 1 bietet dem Benutzer vorteilhafterweise auch die Möglichkeit, die Datenübertragung bei Anzeige einer hohen Datenübertragungsrate durch die LED der Anzeigeeinheit 15 zu unterbrechen. Dies kann beispielsweise über eine Berührungs-Eingabe über eine graphische Benutzeroberfläche auf dem Display der Anzeigeeinheit 15 erfolgen. Als einfachere Ausführungsvariante ist beispielsweise auch ein Betätigen eines Drückknopfes der Anzeigeeinheit 15 zur Unterbrechung der Datenübertragung denkbar.

[0046] Alternativ kann vorgesehen sein, dass eine maximale Datenmenge pro Zeiteinheit und/oder eine Anzahl von Dateien pro Zeiteinheit als Grenzwert der Datenübertragungsrate vorgegeben wird und die Zugriffssteuerungseinheit 1 die Datenübertragung bei Überschreiten der vorgegebenen Parameter automatisch abbricht. Allenfalls kann dieser Grenzwert auch in Abhängigkeit von einer Uhrzeit vorgegeben werden.

[0047] Dieser Grenzwert kann alternativ oder zusätzlich auch stufenweise vorgegeben werden, sodass bei Überschreitung eines ersten vorgegebenen Grenzwerts der Datenübertragungsrate zuerst ein Alarmhinweis von der Zugriffssteuerungseinheit 1 angezeigt wird und bei Überschreitung eines über dem ersten Grenzwert liegenden zweiten Grenzwerts die Zugriffssteuerungseinheit 1 die Datenübertragung automatisch abbricht.

[0048] Weiters gilt für alle Ausführungsformen, dass die Schlüsseleingabeeinheit 13 zur Eingabe oder Erfassung eines Schlüssels S einer der folgenden Arten ausgebildet ist:
- Einlesen des den Schlüssel S enthaltenden zweidimensionalen Codes, beispielsweise eines Barcodes oder QR-Codes, mittels einer optischen Leseeinheit,
- Einlesen eines Schlüssels S von einem Datenträger, z. B. von einem USB-Stick,
- Einlesen des Schlüssels S von einem NFC-fähigen Hardware-Item mittels NFC,
- Manuelle Eingabe des Schlüssels S durch einen Benutzer.

Es kann vorteilhafterweise auch vorgesehen sein, dass die Schlüsseleingabeeinheit 13 der Zugriffssteuerungseinheit 1 auch die Eingabe oder Erfassung verschiedener Arten von Schlüsseln S ermöglicht.

[0049] Alternativ kann bei allen voranstehend beschriebenen Varianten, wie in Fig. 4 dargestellt, auch vorgesehen sein, dass die erste physikalische Schnittstelle 11 der Zugriffssteuerungseinheit 1 auf mehrere auf einem Datenspeicher 2 abgespeicherte Container C zugreifen kann. Dabei kann für alle Container C_1, C_2,... ein Schlüssel S verwendet werden, es kann aber vorteilhafterweise auch vorgesehen sein, dass die in verschiedenen Containern C_1, C_2,... gespeicherten verschlüsselten Daten DV_1, DV_2,... mit verschiedenen Schlüsseln S_1, S_2,... verschlüsselt sind. Die Schlüsseleingabeeinheit 14 ermöglicht in diesem Fall die Eingabe mehrerer verschiedener Schlüssel S_1, S_2,..., wobei der Prozessor 14 die Schlüssel S_1, S_2,..., den gespeicherten verschlüsselten Daten DV_1, DV_2,... zuordnet. Der Rechner 3 kann nun auf jedes der einzelnen virtuellen Laufwerke über die zweite Schnittstelle 12 zugreifen. Dabei besteht die Möglichkeit weiterer Konfigurationen, beispielsweise von Schreib- und Leserechten und anderen Berechtigungen, die für jeden einzelnen Container C separat vorgenommen werden können.

[0050] Alternativ kann auch vorgesehen sein, dass die erste physikalische Schnittstelle 11 der Zugriffssteuerungseinheit 1 auf einen auf mehrere Datenspeicher 2, 2a, ... verteilten Container C zugreifen kann, wobei die im Container C gespeicherten verschlüsselten Daten DV mehrfach auf den verschiedenen Datenspeichern 2, 2a, ... vorkommen können. Eine derartige Organisation des Containers C und der darauf gespeicherten verschlüsselten Daten DV gewährleistet

vorteilhafterweise eine höhere Ausfallsicherheit und/oder einen größeren Datendurchsatz als bei Verwendung eines einzelnen physischen Datenspeichers 2.

[0051] Bei Vorliegen einer Leseanfrage werden einzelne denselben Container C betreffende Datenspeicher 2, 2a ausgelesen, die sich auf die in der Leseanfrage genannten Daten beziehen. Dies wird entsprechend der für die verteilte Speicherung vorgegebenen logischen Zuordnung vorgenommen. Die so erhaltenen Speicherwerte werden aufgrund des Schlüssels zu entschlüsselt und an die zweite Schnittstelle weitergeleitet.

[0052] Bei Vorliegen einer Schreibanfrage werden die zu schreibenden Daten mit dem Schlüssel verschlüsselt. Die derart ermittelten Verschlüsselungsergebnisse werden auf einzelne denselben Container (C) betreffende Datenspeicher (2, 2a) geschrieben.

[0053] Bei allen Ausführungsformen kann alternativ auch vorgesehen sein, dass die Zugriffssteuerungseinheit 1 zumindest eine weitere physikalische Schnittstelle 11a zum Anschluss an einen weiteren Datenspeicher 2a vorgesehen ist, die den Zugriff auf zumindest einen weiteren Container C auf dem Datenspeicher 2a ermöglicht (Fig. 4).

Patentansprüche

1. Zugriffssteuerungseinheit (1) zur Steuerung des Zugriffs auf in einem Datenspeicher (2) gespeicherte verschlüsselte Daten (DV), umfassend eine erste physikalische Schnittstelle (11) zum Anschluss an zumindest einen Datenspeicher (2), eine zweite physikalische Schnittstelle (12) zum Anschluss an einen Rechner (3), eine Schlüsseleingabeeinheit (13) und einen Prozessor (14)
   - wobei die erste physikalische Schnittstelle (11) zum Zugriff auf zumindest einen auf zumindest einem Datenspeicher (2) abgespeicherten Container (C) ausgebildet ist,
   - wobei die Zugriffssteuerungseinheit (1) dazu ausgebildet ist, über die zweite physikalische Schnittstelle (12) nach einem vorgegebenen Protokoll Zugriff auf ein virtuelles Laufwerk zu gewähren,
   - wobei die Schlüsseleingabeeinheit (13) zur Eingabe eines Schlüssels (S) durch einen Benutzer ausgebildet ist,
   - wobei der Prozessor (14) dazu ausgebildet ist, bei Vorliegen einer Leseanfrage (L) an der zweiten physikalischen Schnittstelle (12) eine diesbezügliche Zugriffsanfrage an der ersten physikalischen Schnittstelle (11) bereitzustellen und über die zweite physikalische Schnittstelle (12) auf die in zumindest einem Container (C) auf dem zumindest einen Datenspeicher (2) gespeicherten Daten (DV) zuzugreifen und den Inhalt des Containers (C) mit dem Schlüssel (S) zu entschlüsseln und an der zweiten physikalischen Schnittstelle (12) bereitzustellen.

2. Zugriffssteuerungseinheit (1) nach Anspruch 1, **dadurch gekennzeichnet**, dass der Prozessor (14) dazu ausgebildet ist, bei Vorliegen eines Schreibanfrage (W) die zu schreibenden Daten (D1, D2,...) zu verschlüsseln und im Container (C) auf dem Datenspeicher (2) abzuspeichern.

3. Zugriffssteuerungseinheit (1) nach Anspruch 1 oder 2, **dadurch gekennzeichnet**, dass der Prozessor (14) zur Überwachung des Datenverkehrs über die zweite Schnittstelle und zur Erstellung eines Alarmhinweises ausgebildet ist, wenn die Datenübertragungsrate oder die Rate der pro Zeiteinheit übertragenen Dateien einen vorgegebenen ersten Grenzwert überschreitet, und
   - dass die Zugriffssteuerungseinheit eine Anzeigeeinheit (15) zur Anzeige eines solchen Alarmhinweises umfasst und der Prozessor (14) dazu ausgebildet ist, in diesem Fall dem Benutzer die Möglichkeit zum manuellen Unterbrechung der Datenübertragung zu ermöglichen, und/oder
   - dass der Prozessor (14) dazu ausgebildet ist, bei Überschreiten eines den ersten Grenzwert übersteigenden vorgegebenen zweiten Grenzwerts die Datenübertragung zu unterbrechen.

4. Zugriffssteuerungseinheit (1) nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet**, dass die erste physikalische Schnittstelle (11) zum Zugriff auf mehrere auf einem Datenspeicher (2) abgespeicherten Container (C_1, C_2,...) ausgebildet ist,
   wobei die in den jeweiligen Containern (C_1, C_2,...) gespeicherten Daten (DV_1, DV_2,...) vorzugsweise mit verschiedenen Schlüsseln (S_1, S_2,...) verschlüsselt sind und die Schlüsseleingabeeinheit (13) die Eingabe mehrerer Schlüssel (S_1, S_2,...) ermöglicht und wobei der Prozessor (14) die Zuordnung der Schlüssel (S_1, S_2,...) zu den zugehörigen verschlüsselten Daten (DV_1, DV_2,...) ermöglicht.

5. Zugriffssteuerungseinheit (1) nach einem der Ansprüche 1 bis 4, **dadurch gekennzeichnet**, dass zumindest eine weitere physikalische Schnittstelle (11a) zum Anschluss an zumindest einen weiteren Datenspeicher (2a) sowie zum Zugriff auf zumindest einen weiteren Container (C) auf dem Datenspeicher (2a) vorgesehen ist.

6. Zugriffssteuerungseinheit (1) nach einem der Ansprüche 1 bis 5, **dadurch gekennzeichnet**, dass die erste physikalische Schnittstelle (11) zum Zugriff auf einen auf mehrere Datenspeicher (2, 2a,...) verteilt gespeicherten Container (C) ausgebildet ist, wobei der Prozessor (14) dazu ausgebildet ist, entsprechend der für die verteilte Speicherung vorgege-

benen logische Zuordnung
bei Vorliegen einer Leseanfrage einzelne denselben Container (C) betreffende Datenspeicher (2, 2a) auszulesen und die so erhaltenen Speicherwerte aufgrund des Schlüssels zu entschlüsseln und an die zweite Schnittstelle weiterzuleiten, und
insbesondere bei Vorliegen einer Schreibanfrage die zu schreibenden Daten mit dem Schlüssel zu verschlüsseln und die derart ermittelten Verschlüsselungsergebnisse auf einzelne denselben Container (C) betreffende Datenspeicher (2, 2a) zu schreiben.

7. Zugriffssteuerungseinheit (1) nach einem der Ansprüche 1 bis 6, **dadurch gekennzeichnet**, dass die Schlüsseleingabeeinheit (13) zur Eingabe oder Erfassung eines Schlüssels S zumindest einer der folgenden Arten ausgebildet ist:
- Einlesen des den Schlüssel (S) enthaltenden zweidimensionalen Codes, insbesondere Barcodes oder QR-Codes, mittels einer optischen Leseeinheit,
- Einlesen eines Schlüssels (S) von einem Datenträger, z. B. von einem USB-Stick,
- Einlesen des Schlüssels (S) von einem NFC-fähigen Hardware-Item mittels NFC,
- Manuelle Eingabe des Schlüssels (S) durch einen Benutzer.

8. Speichereinheit (5) umfassend eine Zugriffssteuerungseinheit (1) nach einem der Ansprüche 1 bis 7 sowie zumindest einen Datenspeicher (2), wobei der Datenspeicher (2) über die erste physikalische Schnittstelle (11) an die Zugriffssteuerungseinheit (1) angeschlossen ist.

9. System (6) umfassend eine Speichereinheit (5) nach Anspruch 8 sowie einen Rechner (3), wobei der Rechner (3) über die zweite physikalische Schnittstelle (12) an die Zugriffssteuerungseinheit (1) angeschlossen ist.

10. Verfahren für ein System (6) nach Anspruch 9 zum Zugriff eines Rechners (3) auf in einem Datenspeicher (2) gespeicherte verschlüsselte Daten (DV) mittels einer Zugriffssteuerungseinheit (1),
- wobei die Zugriffssteuerungseinheit (1) einen durch einen Benutzer eingegebenen Schlüssel (S) ermittelt,
- wobei der Rechner (3) eine Leseanfrage (L) über die zweite physikalische Schnittstelle (12) an die Zugriffssteuerungseinheit (1) übermittelt,
- wobei die Zugriffssteuerungseinheit (1) die Leseanfrage (Z) an den Datenspeicher (2) weiterleitet,
- wobei der Datenspeicher (2) die der Leseanfrage (Z) entsprechenden verschlüsselten Daten (DV) an die Zugriffssteuerungseinheit (1) übermittelt,
- wobei die Zugriffssteuerungseinheit (1) die vom Datenspeicher (2) übermittelten verschlüsselten Daten (DV) mit dem Schlüssel (S) entschlüsselt,
- wobei die Zugriffssteuerungseinheit (1) die entschlüsselten Daten (D) über die zweite physikalische Schnittstelle (12) an den Rechner (3) übermittelt.

11. Verfahren nach Anspruch 10, wobei der Rechner (3) eine Schreibanfrage (W) und auf den Datenspeicher (2) zu speichernde Daten (D) über die zweite physikalische Schnittstelle (12) an die Zugriffssteuerungseinheit (1) übermittelt,
- wobei die Zugriffssteuerungseinheit (1) die vom Rechner (3) übermittelten Daten (D) mit dem Schlüssel (S) verschlüsselt,
- wobei die Zugriffssteuerungseinheit (1) die verschlüsselten Daten (DV) und die Schreibanfrage (Z') über die erste physikalische Schnittstelle (11) an den Datenspeicher (2) übermittelt.
- wobei die verschlüsselten Daten (DV) in einem Container (C) auf dem Datenspeicher (2) gespeichert werden.

12. Verfahren nach Anspruch 10 oder 11, **dadurch gekennzeichnet**, dass die Zugriffssteuerungseinheit (1) der Datenverkehr über die zweite Schnittstelle überwacht,
- wobei bei Überschreiten eines vorgegebenen ersten Grenzwerts der Datenübertragungsrate ein Alarmhinweis von der Zugriffssteuerungseinheit (1) erzeugt und angezeigt wird dem Benutzer die Möglichkeit zur Unterbrechung des Datenverkehrs über die erste

Schnittstelle geboten wird und/oder
- wobei die Datenübertragung über die zweite Schnittstelle bei Überschreiten eines vorgegebenen den ersten Grenzwert überschreitenden zweiten Grenzwerts die, insbesondere ohne erforderliche Benutzerinteraktion, unterbrochen wird.

13. Verfahren nach einem der Ansprüche 10 bis 12, **dadurch gekennzeichnet**, dass der erste und/oder zweite Grenzwert der Datenübertragungsrate vorgegeben wird als eine maximale Datenmenge pro Zeiteinheit und/oder eine Anzahl von Dateien pro Zeiteinheit, wobei insbesondere
- der erste und/oder zweite Grenzwert abhängig von einer Uhrzeit vorgegeben wird.

14. Verfahren nach einem der Ansprüche 10 bis 13, **dadurch gekennzeichnet**, dass die Zugriffssteuerungseinheit (1) auf einen auf mehrere Datenspeicher (2, 2a,...) verteilten Container (C) zugreift.

Hierzu 4 Blatt Zeichnungen

1/4

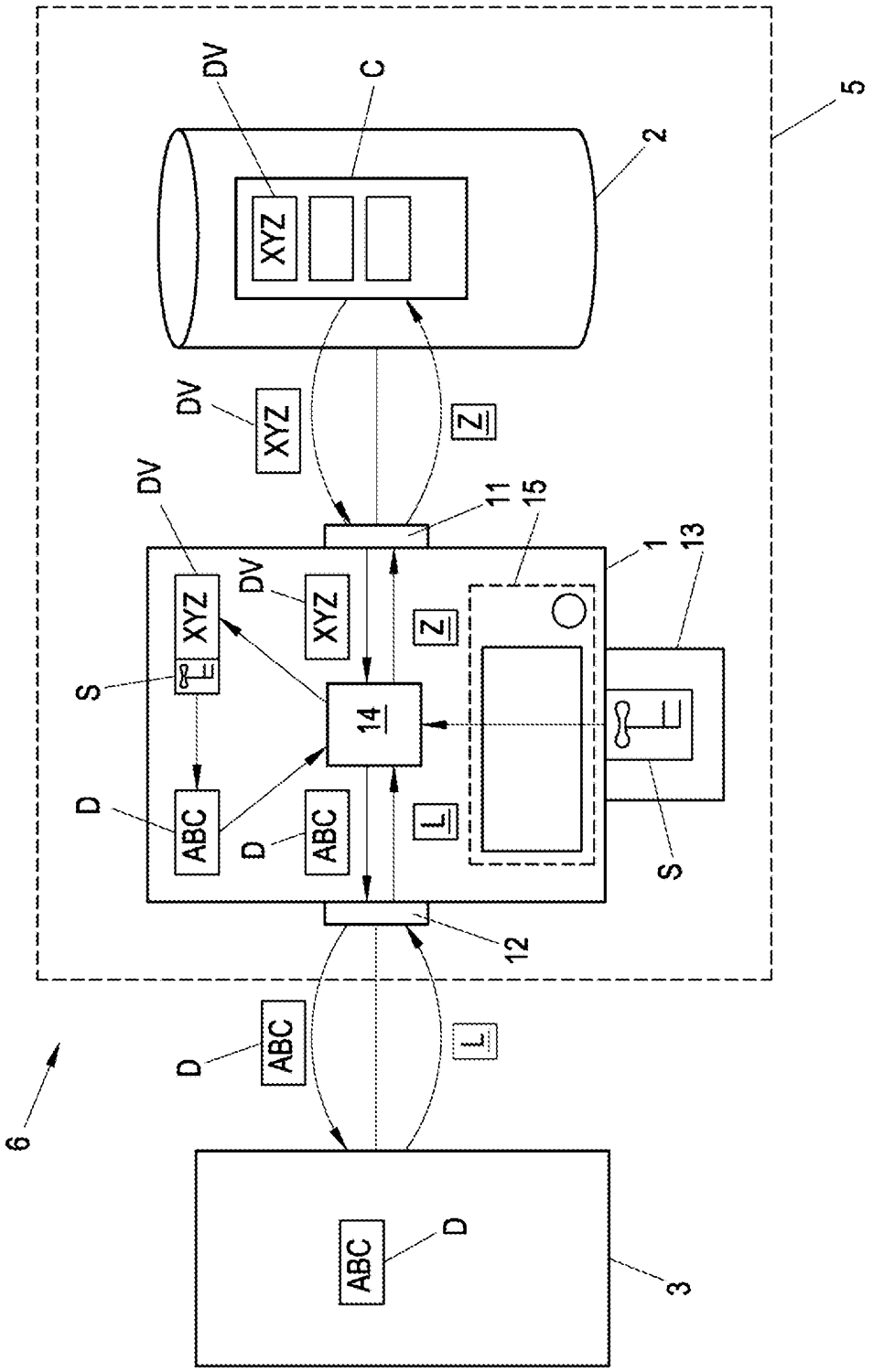
DV
C
5
2
XYZ
DV
XYZ
Z
DV
11
15
1
13
DV
XYZ
XYZ
Z
S
L
14
D
ABC
D
ABC
L
S
12
6
D
ABC
L
ABC
D
3

Fig. 1

2/4

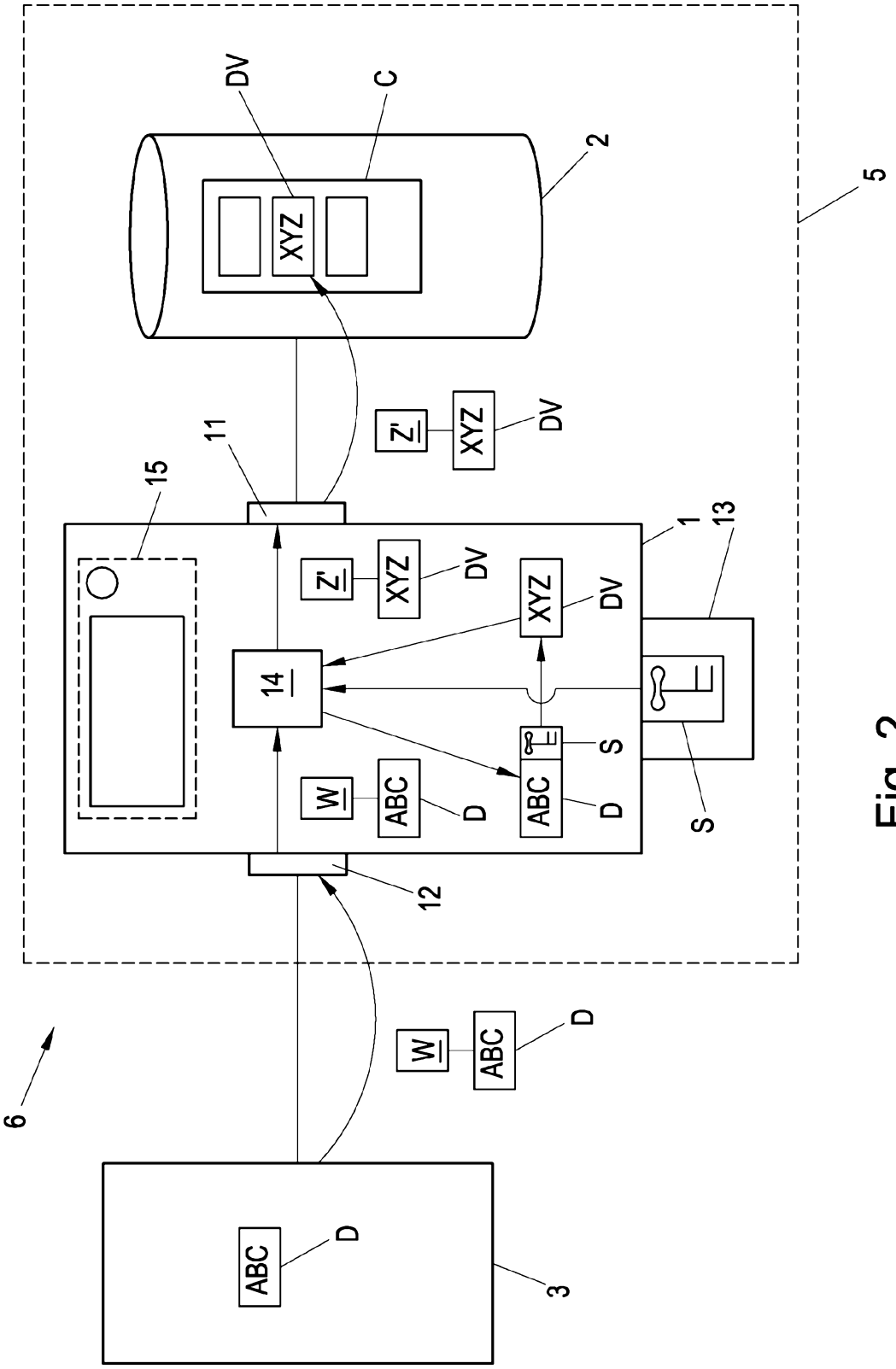
DV
C
2
XYZ
5
Z'
XYZ
DV
11
15
1
13
Z'
XYZ
DV
XYZ
DV
14
S
W
ABC
D
ABC
D
S
12
W
ABC
D
6
ABC
D
3

Fig. 2

3/4

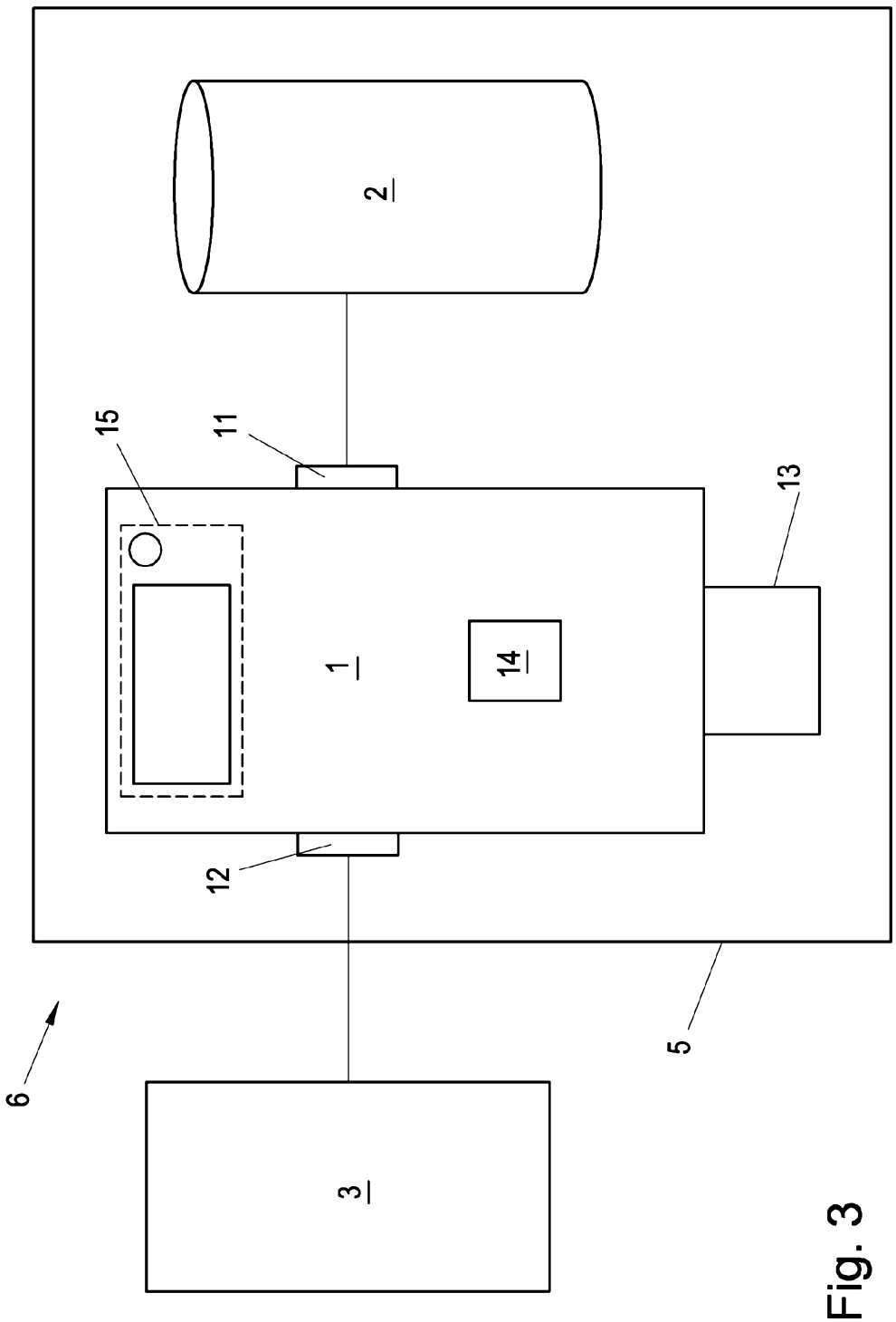

Fig. 3

4/4

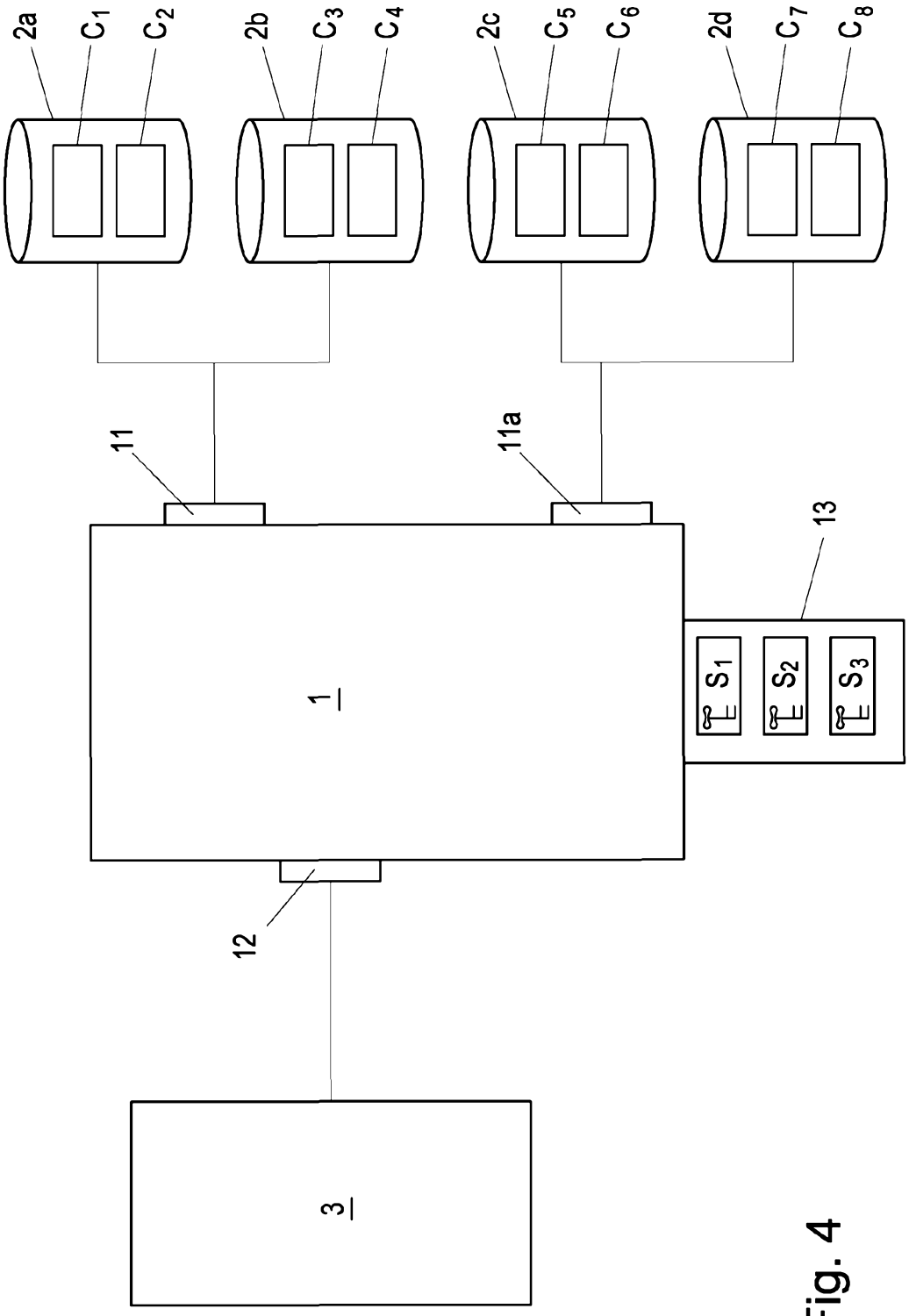

Fig. 4