

(19)



österreichisches
patentamt

(10)

AT 500 264 A2 2005-11-15

(12)

Österreichische Patentanmeldung

(21) Anmeldenummer:

A 2054/2004

(51) Int. Cl.⁷: G06F 12/14

(22) Anmeldetag:

07.12.2004

(43) Veröffentlicht am:

15.11.2005

(30) Priorität:

30.12.2003 DE 10361800 beansprucht.

(73) Patentanmelder:

SIEMENS AKTIENGESELLSCHAFT
D-80333 MÜNCHEN (DE)

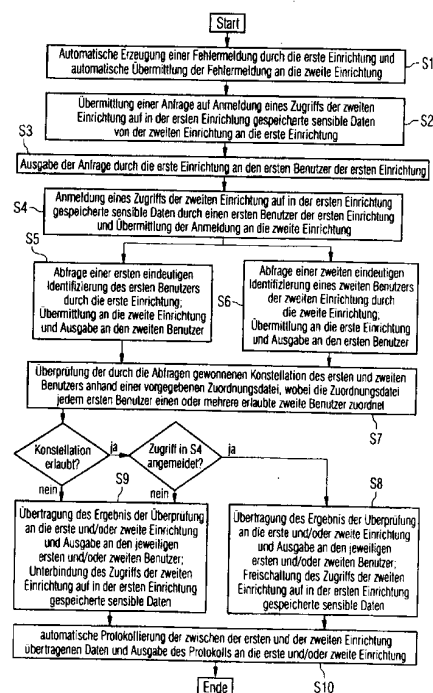
(72) Erfinder:

BIEBER BERNT
HAUSEN (DE)
WESLOH DIRK
ERLANGEN (DE)

(54) VERFAHREN ZUR STEUERUNG

(57) Das Verfahren zur Steuerung des Zugriffs auf in einer Einrichtung 1 gespeicherte sensible Daten 4 durch eine mit der ersten Einrichtung verbundene Einrichtung 2, weist die folgenden Schritte auf:

- (S4) Anmeldung eines Zugriffs der Einrichtung 2 durch einen Benutzer 5 der Einrichtung 1 und Übermittlung der Anmeldung an die Einrichtung 2;
- (S5) Abfrage einer eindeutigen Identifizierung des Benutzers 5 durch die Einrichtung 1;
- (S6) Abfrage einer eindeutigen Identifizierung eines Benutzers 6 der zweiten Einrichtung 2 durch die Einrichtung 2;
- (S7) Überprüfung der durch die Abfragen gewonnenen Konstellation des ersten und zweiten Benutzers 5, 6 anhand einer Zuordnungsdatei 7, wobei die Zuordnungsdatei 7 jedem Benutzer 5 einen oder mehrere erlaubte Benutzer 6, 6', 6'' zuordnet;
- (S8) Freischaltung des Zugriffs wenn die Überprüfung eine erlaubte Konstellation feststellt;
- (S9) Unterbindung des Zugriffs wenn die Überprüfung keine erlaubte Konstellation feststellt oder ein Zugriff der Einrichtung 2 durch den ersten Benutzer 5 nicht angemeldet wurde.



AT 500 264 A2 2005-11-15

Zusammenfassung

Das erfindungsgemäße Verfahren zur Steuerung des Zugriffs auf
in einer ersten Einrichtung 1 gespeicherte sensiblen Daten 4
5 durch eine mit der ersten Einrichtung verbundene zweite Ein-
richtung 2, weist die folgenden Schritte auf:

- (S4) Anmeldung eines Zugriffs der zweiten Einrichtung 2 auf
in der ersten Einrichtung 1 gespeicherte sensible Daten 4
durch einen ersten Benutzer 5 der ersten Einrichtung 1 und
10 Übermittlung der Anmeldung an die zweite Einrichtung 2;
- (S5) Abfrage einer ersten eindeutigen Identifizierung des
ersten Benutzers 5 durch die erste Einrichtung 1;
- (S6) Abfrage einer zweiten eindeutigen Identifizierung ei-
nes zweiten Benutzers 6 der zweiten Einrichtung 2 durch die
15 zweite Einrichtung 2;
- (S7) Überprüfung der durch die Abfragen gewonnenen Konstel-
lation des ersten und zweiten Benutzers 5, 6 anhand einer
vorgegebenen Zuordnungsdatei 7, wobei die Zuordnungsdatei 7
jedem ersten Benutzer 5 einen oder mehrere erlaubte zweite
20 Benutzer 6, 6', 6'' zuordnet;
- (S8) Freischaltung des Zugriffs der zweiten Einrichtung 2
auf in der ersten Einrichtung 1 gespeicherte sensible Da-
ten 4, wenn die Überprüfung der Zuordnung eine erlaubte Kons-
tellation von erstem und zweitem Benutzer 5, 6 feststellt;
- 25 - (S9) Unterbindung des Zugriffs der zweiten Einrichtung 2
auf in der ersten Einrichtung 1 gespeicherte sensible Da-
ten 4, wenn die Überprüfung der Zuordnung keine erlaubte
Konstellation von erstem und zweitem Benutzer 5, 6 feststellt
oder ein Zugriff der zweiten Einrichtung 2 auf in der ersten
30 Einrichtung 1 gespeicherte sensible Daten 4 durch den ersten
Benutzer 5 nicht angemeldet wurde.

(Fig. 3)

Wien, am 07. Dez. 2004

SIEMENS AKTIENGESELLSCHAFT

durch:

Häupl & Eilmeyer KEG

Moderne technische Einrichtungen und insbesondere medizinische Geräte (z.B. Kernspintomographen) weisen eine hohe Komplexität auf. Hierdurch ist es beispielsweise bei der Fehlfunktion eines Kernspintomographen häufig nicht ausreichend, einen einzelnen, allgemein qualifizierten Mitarbeiter zur Behebung des Fehlers heranzuziehen. Vielmehr ist es vielfach erforderlich, aus einem Pool hochqualifizierter Experten den für die Behebung des jeweiligen Fehlers spezialisierten Experten heranzuziehen.

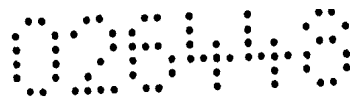
Dies ist besonders bei einer räumlich verteilten Anordnung der technischen Einrichtungen problematisch, da solche hochqualifizierten Experten nicht an allen Orten gleichermaßen verfügbar sind.

Zudem müssen die hochqualifizierten Mitarbeiter im Falle einer Fehlermeldung bei einer räumlich verteilten Anordnung hochentwickelter technischer Einrichtungen oft große Wege zurücklegen, um eine fehlerhafte technische Einrichtung zu reparieren.

Die langen Anfahrtszeiten der für die Reparatur ausgeschickten Experten haben entsprechend lange Ausfallzeiten der jeweiligen technischen Einrichtungen zur Folge.

In diesem Zusammenhang ist zu betonen, dass derartige technische Einrichtungen häufig durch komplexe Softwareprogramme gesteuert werden. Die hohe Komplexität der verwendeten Software führt dazu, dass ein Großteil der Störungen von komplexen technischen Einrichtungen wie z.B. Kernspintomographen weniger auf Materialfehler als vielmehr auf Softwarefehler zurückzuführen sind.

35



Zur Lösung dieser Problematik ist es im Stand der Technik bekannt, eine Fehlerbehebung einer softwaregesteuerten komplexen technischen Einrichtung durch Fernwartung durchzuführen.

- 5 Hierfür ist die technische Einrichtung beispielsweise über das Internet mit einem Servicecenter verbunden, an dem eine Vielzahl von hochqualifizierten Mitarbeitern versammelt ist.

10 Im Falle einer Störung schickt die technische Einrichtung automatisch eine Fehlermeldung an das Servicecenter.

Die an dem Servicecenter versammelten Experten analysieren die Störung anhand der übermittelten Fehlermeldung und versuchen die Störung durch Überspielung einer korrigierten Software an die technische Einrichtung über das Internet zu beheben.

15

Das Dokument **US 2003/0154274 A1** offenbart ein System, das einen effizienten Datenaustausch innerhalb eines Netzwerkes bei der Verwendung von portablen Datenstationen erlaubt. Das System enthält eine erste Datenstation, die bestimmte Daten speichert, sowie eine zweite Datenstation, welche Zugriffsrechte auf die in der ersten Datenstation gespeicherten Daten kontrolliert. Die zweite Datenstation ermächtigt weitere Datenstationen zum Zugriff auf gewünschte Daten. Hierfür erhält die erste Datenstation eine Anfrage in Form eines Datenzeichens (token) und gibt unter der Voraussetzung, dass das Datenzeichen gültig ist, die entsprechenden Daten an den Antragsteller aus. Zur Erstellung eines derartigen Datenzeichens ist erforderlich, dass ein Benutzer der ersten Datenstation mit einem Benutzer einer anfragenden Datenstation ausdrücklich über den jeweiligen Datenaustausch übereinkommt.

20

25

30

Aufgrund der in vielen Ländern geltenden rechtlichen Rahmenbedingungen ist es jedoch derzeit nicht möglich, ein Fernwartungssystem auch für medizinische Geräte einzusetzen, da medizinische Geräte in aller Regel sensible Patientendaten ent-

35

halten können und damit strengen Datenschutzvorschriften unterliegen.

5 Derartige sensible Patientendaten dürfen beispielsweise gemäß der Rechtslage in Deutschland nur dem jeweiligen Arzt oder einem dem Betrieb des Arztes zuzuordnenden Gehilfen des Arztes zugänglich gemacht werden.

10 Um als Gehilfe des Arztes im Sinne der rechtlichen Vorschriften zu gelten, muss ein für die Fehlerbehebung des medizinischen Gerätes eingesetzter Experte dem Arzt bekannt und die Gesamtzahl der für den Arzt zuständigen Experten stark begrenzt sein. Nur in diesem Fall kann von einer Einbindung des jeweiligen Experten in die Organisation des Arztes ausgegan-
15 gen werden kann, wodurch einen Zugriff auf sensible Patientendaten zulässig wird.

Aufgrund der entsprechenden Vorschriften des Datenschutzes treten derartige sensible Daten jedoch nicht nur im Bereich
20 der Medizin sondern auch in anderen Bereichen auf.

Es ist daher Aufgabe der vorliegenden Erfindung, ein Verfahren und eine Anordnung zur Steuerung des Zugriffes auf in einer technischen Einrichtung gespeicherte sensible Daten be-
25 reitzustellen, welche auf besonders einfache und gleichwohl zuverlässige Weise sicherstellt, dass nur von einem jeweiligen Benutzer der technischen Einrichtung legitimierte Personen Zugriff auf die sensible Daten erhalten können.

30 Die Aufgabe wird gemäß den Merkmalen der unabhängigen Ansprüche 1 und 17 gelöst. Die Erfindung wird in den jeweiligen Unteransprüchen weitergebildet.

Gemäß der vorliegenden Erfindung weist ein Verfahren zur
35 Steuerung des Zugriffs auf in einer ersten Einrichtung gespeicherte sensible Daten durch eine mit der ersten Einrich-

tung verbundene zweite Einrichtung die folgenden Schritte auf:

- Anmeldung eines Zugriffs der zweiten Einrichtung auf in der ersten Einrichtung gespeicherte sensible Daten durch einen ersten Benutzer der ersten Einrichtung und Übermittlung der Anmeldung an die zweite Einrichtung;
- Abfrage einer ersten eindeutigen Identifizierung des ersten Benutzers durch die erste Einrichtung;
- Abfrage einer zweiten eindeutigen Identifizierung eines zweiten Benutzers der zweiten Einrichtung durch die zweite Einrichtung;
- Überprüfung der durch die Abfragen gewonnenen Konstellation des ersten und zweiten Benutzers anhand einer vorgegebenen Zuordnungsdatei, wobei die Zuordnungsdatei jedem ersten Benutzer einen oder mehrere erlaubte zweite Benutzer zuordnet;
- Freischaltung des Zugriffs der zweiten Einrichtung auf in der ersten Einrichtung gespeicherte sensible Daten, wenn die Überprüfung der Zuordnung eine erlaubte Konstellation von erstem und zweitem Benutzer feststellt; und
- Unterbindung des Zugriffs der zweiten Einrichtung auf in der ersten Einrichtung gespeicherte sensible Daten, wenn die Überprüfung der Zuordnung keine erlaubte Konstellation von erstem und zweitem Benutzer feststellt oder ein Zugriff der zweiten Einrichtung auf in der ersten Einrichtung gespeicherte sensible Daten durch den ersten Benutzer nicht angemeldet wurde.

Da gemäß dem erfindungsgemäßen Verfahren ein Zugriff auf in der ersten Einrichtung gespeicherte sensible Daten nur nach Anmeldung durch den ersten Benutzer möglich ist, behält der erste Benutzer die absolute Kontrolle über die sensiblen Daten.

Durch die eindeutige Identifizierung von sowohl dem (ersten) Benutzer der ersten Einrichtung als auch dem (zweiten) Benutzer der zweiten Einrichtung wird vor Freischaltung eines Zugriffes auf sensible Daten sichergestellt, dass der (zwei-

te) Benutzer der zweiten Einrichtung einem vorgegebenen Kreis von Personen angehört, die von dem jeweiligen (ersten) Benutzer der ersten Einrichtung zum Zugriff auf die sensiblen Daten ermächtigt sind.

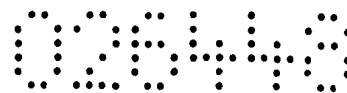
5

Durch die erfindungsgemäße Verwendung einer Zuordnungsdatei kann der für einen Zugriff auf die sensiblen Daten legitimierte Kreis an (zweiten) Benutzern auf besonders einfache Weise für einen jeweiligen ersten Benutzer festgelegt und an diesen angepasst werden. Dies ist insbesondere bei ersten technischen Einrichtungen, die von einer Vielzahl von ersten Benutzern genutzt werden, von erheblicher Bedeutung, um eine Fernwartung zu ermöglichen.

15 Der Zugriff auf eine vorgegebene Zuordnungsdatei, in der für jeden ersten Benutzer ein oder mehrere erlaubte zweite Benutzer zugeordnet sind, weist zudem eine hohe Transparenz und Rechtsicherheit auf, die es einem ersten Benutzer auf besonders einfache Art und Weise durch Auslesen der Zuordnungsdatei ermöglicht, einen ständigen Überblick über für einen Zugriff von sensiblen Daten des jeweiligen ersten Benutzers legitimierte zweite Benutzer zu behalten.

25 Zusammenfassend kann mit Hilfe des erfindungsgemäßen Verfahrens auch bei (ersten) technischen Einrichtungen, auf denen sensible Daten gespeichert sind, eine Fernwartung mittels zweiter technischer Einrichtungen durchgeführt werden. Hierdurch können die mit der Fernwartung verbundenen Vorteile wie eine erhebliche Zeitersparnis bei der Fehlerbehebung und der Verfügbarkeit einer Vielzahl von Experten auch für technische Einrichtungen mit sensiblen Daten genutzt werden.

35 Gemäß einem bevorzugten Ausführungsbeispiel gehen dem Schritt der Anmeldung eines Zugriffs der zweiten Einrichtung auf in der ersten Einrichtung gespeicherte sensible Daten durch den ersten Benutzer die folgenden Schritte voraus:



- Übermittlung einer Anfrage auf Anmeldung eines Zugriffs der zweiten Einrichtung auf in der ersten Einrichtung gespeicherte sensible Daten von der zweiten Einrichtung an die erste Einrichtung; und
- 5 - Ausgabe der Anfrage durch die erste Einrichtung an den ersten Benutzer der ersten Einrichtung.

Dabei ist es besonders vorteilhaft, wenn der Schritt der Übermittlung einer Anfrage auf Anmeldung eines Zugriffs der
10 zweiten Einrichtung auf in der ersten Einrichtung gespeicherte sensible Daten durch die zweite Einrichtung erst nach Erhalt einer von der ersten Einrichtung erzeugten und an die zweite Einrichtung übermittelten Mitteilung erfolgt.

- 15 Hierdurch verbleibt die Kontrolle über die Einleitung des erfindungsgemäßen Verfahrens bei der ersten Einrichtung.

In diesem Fall ist es besonders vorteilhaft, wenn die von der ersten Einrichtung an die zweite Einrichtung übermittelte
20 Mitteilung eine automatisch erzeugte und/oder übermittelte Fehlermeldung ist.

Somit ist sichergestellt, dass eine Anfrage auf Anmeldung eines Zugriffs der zweiten Einrichtung auf in der ersten Einrichtung gespeicherte sensible Daten nur im Falle eines Fehlers bei der ersten Einrichtung möglich ist.
25

Damit nicht auch in Fällen, in denen für eine Fehlerbehebung die Übermittlung von sensiblen Daten gar nicht erforderlich
30 ist, ein Zugriff auf sensible Daten ermöglicht wird, ist es weiter vorteilhaft, wenn der Schritt der Übermittlung einer Anfrage auf Anmeldung eines Zugriffs der zweiten Einrichtung auf in der ersten Einrichtung gespeicherte sensible Daten durch die zweite Einrichtung erst nach einer Überprüfung der
35 Mitteilung durch den Benutzer der zweiten Einrichtung erfolgt.

Um die Fehlertoleranz des erfindungsgemäßen Verfahrens gegen eine Manipulierung der zweiten Einrichtungen zu erhöhen, ist es besonders vorteilhaft, wenn die Abfrage der eindeutigen Identifizierung des zweiten Benutzers der zweiten Einrichtung unter Kontrolle der ersten Einrichtung erfolgt. Dies ist beispielsweise bei der Abfrage eines individuellen Passwortes über ein Datennetzwerk ohne weiteres möglich.

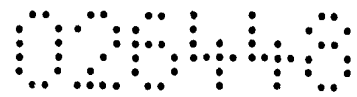
Um dem ersten bzw. zweiten Benutzer der ersten bzw. zweiten Einrichtung Kenntnis über den jeweiligen Benutzer der anderen Einrichtung zu verschaffen ist es vorteilhaft, wenn das Ergebnis der Abfrage der ersten eindeutigen Identifizierung des ersten Benutzers der ersten Einrichtung an die zweite Einrichtung übermittelt und an den zweiten Benutzer ausgegeben wird und/oder das Ergebnis der Abfrage der zweiten eindeutigen Identifizierung des zweiten Benutzers der zweiten Einrichtung an die erste Einrichtung übermittelt und an den ersten Benutzer ausgegeben wird.

Durch Weiterleitung dieser Information an den jeweiligen Benutzer wird die Transparenz des erfindungsgemäßen Verfahrens erhöht, was die Kontrolle durch einen jeweiligen Benutzer verbessert.

Vorzugsweise umfasst die Abfrage einer eindeutigen Identifizierung eines Benutzers die Abfrage eines individuellen Passwortes und/oder eines biometrischen Merkmals und/oder einer elektronischen Signatur und/oder eines individuellen maschinenlesbaren Gegenstandes (beispielsweise einer Magnetkarte oder eines codierten Transponders).

Derartige eindeutige Identifizierungsmöglichkeiten sind dem Benutzer von technischen Geräten allgemein vertraut. Weiter hat sich die Abfrage derartiger eindeutiger Identifizierungsmerkmale von Benutzern in der Praxis als zuverlässig herausgestellt.

- Bevorzugt erfolgt die Überprüfung der durch die Abfrage gewonnenen Konstellation des ersten und zweiten Benutzers gemäß dem erfindungsgemäßen Verfahren wahlweise durch die erste Einrichtung und/oder durch die zweite Einrichtung und/oder
- 5 durch ein oder mehrere mit der ersten und zweiten Einrichtung verbundenen weiteren Einrichtungen, wobei die Zuordnungsdatei in der bzw. den jeweiligen Einrichtungen gespeichert ist.
- Weiter ist es besonders vorteilhaft, wenn das Ergebnis der
- 10 Überprüfung der durch die Abfrage gewonnenen Konstellation des ersten und zweiten Benutzers anhand der Zuordnungsdatei an die erste und/oder zweite Einrichtung übertragen und an den jeweiligen ersten und/oder zweiten Benutzer ausgegeben wird.
- 15 Hierdurch erhalten der erste und/oder zweite Benutzer Kenntnis darüber, ob ein Zugriff auf die sensiblen Daten möglich ist.
- 20 Um die Transparenz des erfindungsgemäßen Verfahrens weiter zu erhöhen und die Kontrolle und Nachvollziehbarkeit der Freigabe von sensiblen Daten sicherzustellen ist es besonders vorteilhaft, wenn das Verfahren weiter den Schritt einer automatischen Protokollierung der zwischen der ersten und der zweiten
- 25 Einrichtung übertragenen Daten und einer Ausgabe des Protokolls an die erste und/oder zweite Einrichtung umfasst.
- Damit in einem Fehlerfall eine zügige Behebung des Fehlers auch durch eine in der Zuordnungsdatei noch nicht in Verbindung mit der jeweiligen ersten Person gespeicherte zweite
- 30 Person möglich ist, weist das erfindungsgemäße Verfahren vorzugsweise zusätzlich den Schritt der Übermittlung eines Genehmigungsformulars an die erste Einrichtung durch die zweite Einrichtung auf.
- 35

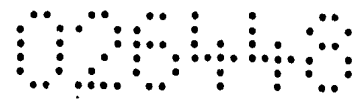


Bevorzugt ist die erste Einrichtung ein medizinisches System und die zweite Einrichtung ein Wartungssystem zur Fernwartung des medizinischen Systems.

- 5 In diesem Falle handelt es sich bei den sensiblen Daten insbesondere um in dem medizinischen System gespeicherte Patientendaten.

10 Die vorstehend angegebene Aufgabe wird erfindungsgemäß auch durch eine Anordnung zur Steuerung des Zugriffs auf in einer ersten Einrichtung gespeicherte sensible Daten durch eine mit der ersten Einrichtung verbundene zweite Einrichtung gelöst, welche die folgenden Merkmale aufweist:

- 15 - eine mit der ersten und zweiten Einrichtung verbundene Datenübertragungseinrichtung zur Übertragung von Daten zwischen der ersten Einrichtung und der zweiten Einrichtung;
- eine mit der ersten Einrichtung verbundene erste Eingabe-
einrichtung zur Anmeldung eines Zugriffs der zweiten Einrichtung auf in der ersten Einrichtung gespeicherte sensible Daten
20 - eine mit der ersten Einrichtung verbundene erste Abfrageeinrichtung zur Abfrage einer ersten eindeutigen Identifizierung des ersten Benutzers durch die erste Einrichtung;
- eine mit der zweiten Einrichtung verbundene zweite Abfrage-
25 einrichtung zur Abfrage einer zweiten eindeutigen Identifizierung eines zweiten Benutzers der zweiten Einrichtung durch die zweite Einrichtung; und
- eine mit der ersten und zweiten Einrichtung verbundene Vergleichseinrichtung zur Überprüfung der von der ersten und
30 zweiten Abfrageeinrichtung gewonnenen Konstellation des ersten und zweiten Benutzers anhand einer vorgegebenen Zuordnungsdatei, wobei die Zuordnungsdatei jedem ersten Benutzer einen oder mehrere erlaubte zweite Benutzer zuordnet und in der Vergleichseinrichtung gespeichert ist,;
- 35 wobei die erste Einrichtung eine Zugriffssteuerungseinrichtung umfasst, die ausgebildet ist, den Zugriff der zweiten Einrichtung auf in der ersten Einrichtung gespeicherte sen-



sible Daten freizugeben, wenn die Vergleichseinrichtung eine erlaubte Konstellation von erstem und zweitem Benutzer feststellt und den Zugriff der zweiten Einrichtung auf in der ersten Einrichtung gespeicherte sensible Daten zu unterbin-

5 den, wenn die Vergleichseinrichtung keine erlaubte Konstellation von erstem und zweitem Benutzer feststellt oder durch die erste Eingabeeinrichtung kein Zugriff der zweiten Einrichtung auf in der ersten Einrichtung gespeicherte sensible Daten angemeldet wurde.

10

Gemäß einer bevorzugten Ausführungsform weist die Anordnung ferner

- eine mit der ersten Einrichtung verbundene Fehlerkontroll-

15 einrichtung zur automatischen Erzeugung und Übermittlung von Fehlermeldungen an die zweite Einrichtung über die Datenübertragungseinrichtung;

- eine mit der zweiten Einrichtung verbundene zweite Ausgabe-

20 einrichtung zur Ausgabe einer von der ersten Einrichtung empfangenen Fehlermeldung an den zweiten Benutzer der zweiten Einrichtung;

- eine zweite Eingabeeinrichtung zur Übermittlung einer Anfrage auf Anmeldung eines Zugriffs der zweiten Einrichtung auf in der ersten Einrichtung gespeicherte sensible Daten nach Erhalt einer von der ersten Einrichtung an die zweite

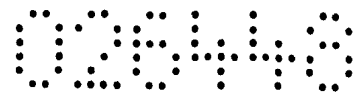
25 Einrichtung übermittelten Fehlermeldung; und

- eine mit der ersten Einrichtung verbundene erste Ausgabe-

einrichtung zur Ausgabe der Anfrage an den ersten Benutzer der ersten Einrichtung auf.

30 Vorzugsweise ist die erste Abfrageeinrichtung ausgebildet, um das Ergebnis der Abfrage der ersten eindeutigen Identifizierung des ersten Benutzers der ersten Einrichtung über die Datenübertragungseinrichtung an die zweite Einrichtung zu übermitteln, und ist die zweite Ausgabeeinrichtung ausgebildet,

35 um das Ergebnis der Abfrage an den zweiten Benutzer auszugeben.



Weiter ist es vorteilhaft, wenn die zweite Abfrageeinrichtung ausgebildet ist, um das Ergebnis der Abfrage der zweiten eindeutigen Identifizierung des zweiten Benutzers der zweiten Einrichtung über die Datenübertragungseinrichtung an die erste Einrichtung zu übermitteln, und ist die erste Ausgabeeinrichtung ausgebildet, um das Ergebnis der Abfrage an den ersten Benutzer auszugeben.

Besonders vorteilhaft ist es, wenn die erste Abfrageeinrichtung und die zweite Abfrageeinrichtung ausgebildet sind, um ein individuelles Passwort und/oder ein biometrisches Merkmal und/oder eine elektronische Signatur und/oder einen individuellen maschinenlesbaren Gegenstand abzufragen.

Es ist ferner vorteilhaft, wenn die Vergleichseinrichtung in der ersten Einrichtung und/oder in der zweiten Einrichtung und/oder durch in einer oder mehreren mit der ersten und zweiten Einrichtung verbundenen weiteren Einrichtungen angeordnet ist.

20

Vorzugsweise ist die Vergleichseinrichtung ferner ausgebildet, das Vergleichsergebnis über die Datenübertragungseinrichtung an die erste und/oder zweite Einrichtung zu übertragen, und ist die erste Ausgabeeinrichtung ausgebildet, um das von der Vergleichseinrichtung gewonnene Vergleichsergebnis an den ersten Benutzer auszugeben, und ist die zweite Ausgabeeinrichtung ausgebildet, um das von der Vergleichseinrichtung gewonnene Vergleichsergebnis an den zweiten Benutzer auszugeben.

30

Bevorzugt weist die Anordnung ferner eine Protokolliereinrichtung auf, um automatisch ein Protokoll der zwischen der ersten und der zweiten Einrichtung übertragenen Daten zu erstellen und das Protokoll über die Datenübertragungseinrichtung an die erste und/oder zweite Einrichtung zu übermitteln.

35

Es ist besonders vorteilhaft, wenn die zweite Einrichtung ferner ausgebildet ist, über die Datenübertragungseinrichtung ein Genehmigungsformular an die erste Einrichtung zu übertragen.

5

Gemäß einer bevorzugten Ausführungsform ist die zweite Einrichtung ein Wartungssystem zur Fernwartung der ersten Einrichtung.

- 10 Dabei ist die erste Einrichtung vorzugsweise ein medizinisches System und die zweite Einrichtung ein Wartungssystem zur Fernwartung des medizinischen Systems.

15 In diesem Falle handelt es sich bei den sensiblen Daten vorzugsweise um in dem medizinischen System gespeicherte Patientendaten.

20 In der folgenden ausführlichen Beschreibung wird die vorliegende Erfindung unter Bezugnahme auf die beigefügten Zeichnungen, in denen gleiche Bezugszeichen auf in den jeweiligen Ansichten gleiche Elemente verweisen, näher beschrieben, wobei

25 Fig. 1 ein Blockdiagramm eines ersten bevorzugten Ausführungsbeispiels der erfindungsgemäßen Anordnung;

Fig. 2 ein Blockdiagramm eines alternativen Ausführungsbeispiels der erfindungsgemäßen Anordnung; und

30 Fig. 3 ein Flußdiagramm des erfindungsgemäßen Verfahrens zeigt.

35 **Figur 1** zeigt ein Blockdiagramm eines ersten bevorzugten Ausführungsbeispiels der erfindungsgemäßen Anordnung zur Steuerung des Zugriffs auf in einer ersten Einrichtung gespeicherte sensible Daten.

Die Anordnung weist eine erste Einrichtung 1 auf, welche gemäß dieser Ausführungsform ein medizinisches System ist. Bei dem medizinischen System 1 kann es sich beispielsweise um einen Kernspintomographen oder einen Computertomographen handeln.

Das medizinische System 1 weist sensiblen Daten 4 auf, die in einem geeigneten Datenträger, beispielsweise einer Festplatte, gespeichert sind. Bei diesen sensiblen Daten handelt es sich gemäß der hier beschriebenen Ausführungsform um Patientendaten und damit beispielsweise um Computer- oder Kernspintomographiebilder von Patienten.

Weiter weist das medizinische System eine Zugriffssteuereinrichtung 13 auf, die ausgebildet ist, um den Zugriff auf die in dem medizinischen System gespeicherten sensiblen Daten 4 freizugeben oder zu unterbinden. In dem vorliegenden Ausführungsbeispiel handelt es sich bei der Zugriffssteuereinrichtung 13 um einen Mikroprozessor, der auf die auf dem Datenträger des medizinischen Systems 1 gespeicherten sensiblen Daten 4 zugreifen kann.

Mit dem medizinischen System 1 ist eine erste Eingabeeinrichtung 9 (in der vorliegenden Ausführungsform eine Tastatur) zur Anmeldung eines Zugriffs auf in der ersten Einrichtung gespeicherte sensible Daten durch einen ersten Benutzer 5 des medizinischen Systems 1 verbunden. Bei dem ersten Benutzer 5 des medizinischen Systems handelt es sich gemäß der vorliegenden Ausführungsform um einen Arzt.

Eine erste Abfrageeinrichtung 11 in Form eines Magnetkartenlesers ist an das medizinische System 1 angeschlossen. Der Magnetkartenlesers 11 ist ausgebildet, um durch Auslesung einer individuellen Magnetkarte des Arztes 5 eine erste eindeutige Identifizierung des Arztes 5 zu ermöglichen.

Weiter sind mit dem medizinischen System 1 eine Fehlerkontrollleinrichtung 14 zur Überwachung der Funktion des medizinischen Systems 1 sowie eine erste Ausgabeeinrichtung 16 zur Ausgabe von von dem medizinischen System 1 empfangenden oder generierten Informationen an den Arzt 5 verbunden.

In der vorliegenden Ausführungsform handelt es sich bei der Fehlerkontrollleinrichtung 14 um einen Mikroprozessor und bei der ersten Ausgabeeinrichtung 16 um einen Monitor.

10

Über eine Datenübertragungseinrichtung 3 ist das medizinische System 1 mit einer zweiten Einrichtung 2, welche ein Wartungssystem zur Wartung des medizinischen Systems 1 ist, verbunden. Die Datenübertragungseinrichtung 3 ermöglicht eine Übertragung von Daten zwischen dem medizinischen System 1 und der Wartungseinrichtung 2.

15

In dem vorliegenden Ausführungsbeispiel handelt es sich bei der Datenübertragungseinrichtung 3 um eine gesicherte Internetverbindung, über die geeignete kodierte Daten zwischen dem medizinischen System 1 und dem Wartungssystem 2 übertragen werden.

20

Das Wartungssystem 2 ist zur Fernwartung des medizinischen Systems 1 über die gesicherte Internetverbindung 3 ausgebildet.

25

Hierfür weist Wartungssystem 2 u.a. eine zweite Abfrageeinrichtung 12 auf, die in dem vorliegenden Ausführungsbeispiel ein Lesegerät für die biometrische Daten eines das Wartungssystem 2 betreuenden Experten 6, 6', 6'' ist.

30

Das Lesegerät für biometrische Daten kann beispielsweise zum Auslesen der Iris oder des Fingerabdruckes des Experten 6, 6', 6'' ausgebildet sein. Somit ermöglicht das Lesegerät für biometrische Daten 12 eine eindeutige Identifizierung eines

35

das Wartungssystem 2 benutzenden Experten 6, 6', 6'' (zweiten Benutzers).

5 Mit dem Wartungssystem 2 sind weiter eine zweite Eingabeeinrichtung 10, bei der es sich beispielsweise um eine Maus handelt, sowie eine zweite Ausgabeeinrichtung 17, bei dem es sich wiederum um einen Monitor handeln kann, verbunden.

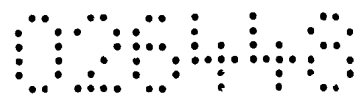
10 Die Maus ermöglicht es dem Experten 6, 6', 6'' das Wartungssystem 2 zu steuern.

Über den Monitor 17 können von dem Wartungssystem 2 generierte oder über die Internetverbindung 3 von dem medizinischen System 1 empfangene Daten an den Experten 6, 6', 6'' ausgegeben werden.

20 Gemäß der vorliegenden bevorzugten Ausführungsbeispiel ist in dem Wartungssystem 2 eine Protokolliereinrichtung 18 in Form eines mit einer Festplatte verbundenen Mikroprozessors angeordnet.

Die Protokolliereinrichtung 18 ist geeignet, automatisch ein Protokoll der zwischen dem medizinischen System 1 und dem Wartungssystem 2 übertragenen Daten zu erstellen, das Protokoll auf der Festplatte zu speichern und über die gesicherte Internetverbindung 3 an das medizinische System 1 zu übermitteln. Das von der Protokolliereinrichtung 18 erzeugte Protokoll kann von dem medizinischen System 1 über den Monitor 16 und von dem Wartungssystem 2 über den Monitor 17 an den Arzt 5 bzw. den Experten 6, 6', 6'' ausgegeben werden. Das Protokoll kann beispielsweise die Namen der am Datenaustausch beteiligten Personen, die Urzeit, die Art des Dateneingriffs (Kopie, Löschung, Einfügung) sowie eine Angabe der jeweiligen Daten enthalten.

35 Die erfindungsgemäße Anordnung zur Steuerung des Zugriffs auf in dem medizinischen System 1 gespeicherte sensible Patienten-



tendaten 4 weist ferner eine über die gesicherte Internetverbindung 3 mit dem medizinischen System 1 und dem Wartungssystem 2 verbundene Vergleichseinrichtung 15 auf.

- 5 In der Vergleichseinrichtung 15 ist eine Zuordnungsdatei 7 abgelegt, in der in tabellarischer Form jedem das medizinische System 1 nutzenden Arzt 5 ein oder mehrere erlaubte Experten 6, 6', 6'' für das Wartungssystem 2 zugeordnet sind.
- 10 Somit ist es der Vergleichseinrichtung 15 anhand der Zuordnungsdatei 7 möglich, eine von dem Magnetkartenleser 11 und dem Lesegerät für biometrische Daten 12 gewonnene Konstellation von Arzt 5 und Experte 6, 6', 6'' auf seine Zulässigkeit zu überprüfen. Hierfür handelt es sich bei der Vergleichseinrichtung 15 vorzugsweise um einen geeigneten Mikroprozessor. Die Zuordnungsdatei 7 kann in einem Festspeichersystem oder einem geeigneten Datenträger gespeichert sein.

- In dem in Fig. 1 gezeigten Ausführungsbeispiel sind zwei Vergleichseinrichtungen 15 vorgesehen, die in zwei weiteren Einrichtungen 8, 8' angeordnet sind. Bei diesen weiteren Einrichtungen 8, 8' handelt es sich um die Datenübertragende überwachende Server die über die gesicherte Internetverbindung mit dem medizinischen System 1 und dem Wartungssystem 2 verbunden sind. Selbstverständlich kann es sich bei den weiteren Einrichtungen 8, 8' auch um andere Systeme handeln.

- Durch die redundante Auslegung der Vergleichseinrichtung 15 können Manipulationen sicher vermieden werden und kann so eine hohe Datensicherheit sichergestellt werden.

- Die Vergleichseinrichtungen 15 der weiteren Einrichtungen 8, 8' sind ausgebildet, um den Zugriff des Wartungssystems 2 auf die in dem medizinischen System 1 gespeicherten Patientendaten 4 durch entsprechende Steuerung der Zugriffssteuereinrichtung 13 freizugeben, wenn anhand der Zuordnungsdatei 7 eine erlaubte Konstellation von Arzt 5 und Experten 6, 6',

6'' festgestellt wurde. Weiter sind die Vergleichseinrichtungen 15 der weiteren Einrichtungen 8, 8' ausgebildet, um den Zugriff des Wartungssystems 2 auf die in dem medizinischen Systems 1 gespeicherten Patientendaten 4 durch entsprechende Steuerung der Zugriffssteuereinrichtung 13 zu unterbinden, wenn die Vergleichseinrichtung 12 keine erlaubte Konstellation von Arzt 5 und Experten 6, 6', 6'' festgestellt hat oder durch die Tastatur 9 kein Zugriff des Wartungssystems 2 auf die in dem medizinischen System 1 gespeicherten Patientendaten 4 angemeldet wurde.

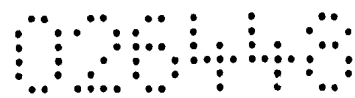
Da für eine Freigabe der Patientendaten immer zunächst eine Anmeldung über das medizinische System 1 erforderlich ist, behält ein das medizinische System 1 bedienender Arzt 5 immer die absolute Verfügungsgewalt über die in dem medizinischen System 1 abgelegten Patientendaten 4.

Über die Vergleichseinrichtungen 15 wird somit sichergestellt, dass lediglich dem Arzt 5 bekannte und von dem Arzt 5 autorisierte Experten 6, 6', 6'', welche dem Betrieb des Arztes zuzurechnen sind, Kenntnis von in dem medizinischen System 1 gespeicherten Patientendaten 4 erlangen können.

Somit ist mit der erfindungsgemäßen Anordnung eine Fernwartung des medizinischen Systems 1 durch das Wartungssystem 2 möglich.

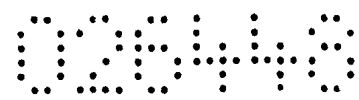
Gemäß dem die Figur 1 bevorzugten Ausführungsbeispiel wird ein Zugriff auf in dem medizinischen System 1 gespeicherte sensible Patientendaten 4 durch die Fehlerkontrolleinrichtung 14 initialisiert, die bei Feststellung eines Fehlers in dem medizinischen System 1 automatisch eine Fehlermeldung erzeugt und über die gesicherte Internetverbindung 3 an das Wartungssystem 3 übermittelt.

35



Die Fehlermeldung wird über den Monitor 17 des Wartungssystems 2 an ein des Wartungssystems 2 bedienenden Experten 6, 6', 6'' ausgegeben.

- 5 Alternativ kann die Fehlermeldung auch manuell durch den Arzt 5 über z.B. eine normale Telephonleitung im Rahmen eines Telefongespräches an das Wartungssystem 3 übermittelt werden.
- 10 Anhand der Fehlermeldung entscheidet der Experte 6, 6', 6'', ob für eine Behebung des Fehlers in dem medizinischen System 1 überhaupt ein Zugriff auf die in dem medizinischen System 1 gespeicherten sensiblen Patientendaten 4 erforderlich ist.
- 15 Kommt der Experte 6, 6', 6'' aufgrund der von der Fehlerkontrollleinrichtung 14 des medizinischen Systems 1 erzeugten und an das Wartungssystem 2 übermittelten Fehlermeldungen zu der Überzeugung, dass für eine Behebung des Fehlers in dem medizinischen Systems 1 ein Zugriff auf sensible Patientendaten 4 erforderlich ist, so übermittelt er über das Wartungssystem 2 und die Datenübertragungseinrichtung 3 eine Anfrage auf Anmeldung eines Zugriffs des Wartungssystems 2 auf die in dem medizinischen System 1 gespeicherten Patientendaten 4.
- 20
- 25 Die Anfrage auf Anmeldung eines Zugriffs des Wartungssystems 2 auf die in dem medizinischen System 1 gespeicherten sensiblen Patientendaten 4 wird dem Arzt 5 über den Monitor 16 des medizinischen Systems 1 angezeigt.
- 30 Der Arzt 5 (oder eine von dem Arzt 5 hierzu legitimierte Person, die in geeigneter Weise in die Organisation des Arztes eingebunden ist) erhält somit nochmals Gelegenheit, über die Einleitung eines Datenaustausches zu entscheiden.
- 35 Um sowohl den das medizinische System 1 bedienenden Arzt 5 als auch den des Wartungssystems 2 bedienenden Experten 6,



6', 6'' über den jeweiligen Bediener des anderen Systems in Kenntnis zu setzten, sind sowohl der Magnetkartenleser 11 als auch das Lesegerät für biometrische Daten 12 ausgebildet, um das Ergebnis der Abfrage der ersten und zweiten eindeutigen Identifizierung des Arztes 5 bzw. des Experten 6, 6', 6'' über die gesicherte Internetverbindung 3 an das jeweilige andere System zu übertragen wo es über den jeweiligen Monitor 16, 17 angezeigt wird.

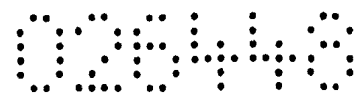
10 Hierdurch ist eine manuelle Überprüfung des jeweiligen Benutzers des jeweiligen Systems durch den jeweiligen anderen Benutzer des anderen Systems möglich.

Um den Arzt 5 und den Experten 6, 6', 6'' von dem jeweiligen Funktionszustand der erfindungsgemäßen Anordnung in Kenntnis zu setzten, sind die Vergleichseinrichtungen 15 ferner ausgebildet, das Ergebnis des Vergleichs über die gesicherte Internetverbindung 3 an das medizinische System 1 und das Wartungssystem 2 zu übertragen wo sie von dem Monitor 16 bzw. dem Monitor 17 an den Arzt 5 bzw. den Experten 6, 6', 6'' ausgegeben werden.

Sollte die von der Vergleichseinrichtung 15 festgestellte Konstellation von Arzt 5 und Experten 6 einen Zugriff auf in dem medizinischen System 1 gespeicherte sensible Patientendaten 4 derzeit nicht zulassen, ist des Wartungssystem 2 gemäß der in Fig. 1 gezeigten Ausführungsform weiter ausgebildet, um über die gesicherte Internetverbindung 3 ein Genehmigungsformular in Form eines Faxformulares an das medizinische System 1 übertragen.

Das Faxformular kann von dem medizinische System 1 über einen in der Figur 1 nicht dargestellten Drucker ausgedruckt werden.

35 Das Genehmigungsformular (Faxformular) ist von dem Arzt 5 entsprechend auszufüllen und unterschrieben an die weiteren



Einrichtungen 8, 8' zu schicken, wo die neue Konstellation von Arzt 5 und Experten 6, 6', 6'' in die jeweilige Zuordnungsdatei 7 eingegeben wird.

5 Somit erlaubt die erfindungsgemäße Anordnung auf einfach und gleichwohl sichere Weise eine flexible Anpassung an die aktuelle Situation, so dass eine Fernwartung eines medizinischen Systems 1 über das Wartungssystem 2 in jedem Fall schnell gewährleistet werden kann.

10

Über das Genehmigungsformular kann durch den Arzt 5 (oder eine vom Arzt legitimierte Person) erforderlichenfalls auch eine Weitergabe der Patienteninformationen 4 durch den Experten 6, 6', 6'' an eine weitere Person legitimiert werden.

15

Figur 2 zeigt ein alternatives Ausführungsbeispiel der erfindungsgemäßen Anordnung zur Steuerung des Zugriffs auf in einer ersten Einrichtung 1 gespeicherte sensible Daten 4 durch eine mit der ersten Einrichtung 1 über eine Datenübertragungseinrichtung 3 verbundene zweite Einrichtung 2 in der gleiche Elemente wie in Figur 1 mit den gleichen Bezugszeichen versehen sind.

20

Das in Figur 2 gezeigte alternative Ausführungsbeispiel unterscheidet sich von dem in Figur 1 gezeigten bevorzugten Ausführungsbeispiel zunächst dadurch, dass die Vergleichseinrichtung 15 und damit die Zuordnungsdatei 7 nicht in einer weiteren Einrichtung 8, 8' angeordnet, sondern in das Wartungssystem 2 integriert ist. Eine Redundanz der Vergleichseinrichtung 15 ist in dem in Figur 2 gezeigten Ausführungsbeispiel somit nicht vorgesehen.

30

Weiter unterscheidet sich das in Figur 2 gezeigte Ausführungsbeispiel von dem in Figur 1 gezeigten Ausführungsbeispiel dadurch, dass die Protokolliereinrichtung 18 nicht in dem Wartungssystem 2 sondern in dem medizinischen System 1

35

angeordnet und die Fehlerkontrolleinrichtung 14 in das medizinische System 1 integriert ist.

Obwohl in den vorstehend beschriebenen Figuren 1 und 2 die Vergleichseinrichtung 15 entweder in separaten weiteren Einrichtungen 8 oder 8' oder in dem Wartungssystem 2 angeordnet ist, ist es selbstverständlich auch möglich, die Vergleichseinrichtung 15 in dem medizinischen System 1 oder sowohl in dem medizinischen System 1 als auch im Wartungssystem 2 vorzusehen.

Weiter ist es alternativ ohne weiteres möglich, anstelle des Magnetkartenlesers 11 und des Lesegeräts für biometrische Daten 12 beliebige Abfrageeinrichtung vorzusehen, die ausgebildet sind, um ein individuelles Passwort und/oder ein biometrisches Merkmal und/oder eine elektronische Signatur und/oder einen individuellen maschinenlesbaren Gegenstand abzufragen.

Bei einem individuellen maschinenlesbaren Gegenstand kann es sich beispielsweise um eine Magnetkarte oder um einen mit einem individuellen Strichcode oder individuell kodierten Transponder versehenen Gegenstand handeln, der geeignet ist, eine Person eindeutig zu identifizieren.

Es ist für den Fachmann offensichtlich, dass die erfindungsgemäße Anordnung nicht nur zur Fernwartung von medizinischen Systemen geeignet ist, sondern beispielsweise auch im Rahmen einer Ferndiagnostik verwendet werden kann. In diesem Fall handelt es sich bei der zweiten Einrichtung 2 um eine Ferndiagnostikeinrichtung, die einen Zugriff auf das medizinische System 1 erlaubt und bei dem die Ferndiagnoseeinrichtung 2 bedienenden zweiten Benutzer 6, 6', 6'' um einen sich der Ferndiagnostikeinrichtung 2 bedienenden zweiten Arzt, der auf die von dem das medizinische System 1 bedienenden ersten Arzt gewonnenen Patientendaten 4 zugreift.

Obwohl in den Figuren 1 und 2 für eine Ausgabe von Daten lediglich Monitore 16 und 17 gezeigt werden, können selbstverständlich beliebige andere Ausgabegeräte für Daten, beispielsweise Drucker etc. verwendet werden. Entsprechend ist auch eine Dateneingabe nicht nur wie in den Figuren 1 und 2 gezeigt über eine Tastatur 9 oder einer Maus 10 möglich, sondern es können beliebige andere Eingabemedien wie z. B. Touchscreens oder Trackballs für eine Dateneingabe verwendet werden.

10

Weiter muss es sich bei der Datenübertragungseinrichtung 3 nicht um eine gesicherte Internetverbindung handeln, sondern es kommen beliebige andere Verbindungen wie beispielsweise eine direkte Verbindung über beispielsweise eine Telefonleitung oder eine gesicherte Leitung oder eine Übertragung über eine Luftschnittstelle in betracht.

15

In dem in den Figs. 1 und 2 gezeigten Ausführungsbeispiel erfolgt die Abfrage von sowohl der ersten als auch der zweiten eindeutigen Identifizierung des ersten und zweiten Benutzers 5, 6, 6', 6'' gleichzeitig durch das medizinische System 1 bzw. die Wartungseinrichtung 2 unter Kontrolle des medizinischen Systems 1. Alternativ kann die Abfrage auch sequentiell und durch Steuerung des Wartungssystems 2 oder getrennt durch das jeweilige System erfolgen.

20

25

Im Folgenden wird das erfindungsgemäße Verfahren zur Steuerung des Zugriffs auf in einer ersten Einrichtung gespeicherte sensible Daten unter Bezugnahme auf Figur 3 näher beschrieben.

30

Wie in **Figur 3** gezeigt wird in einem ersten Schritt S1 automatisch eine Fehlermeldung durch die erste Einrichtung 1 erzeugt und automatisch an die zweite Einrichtung 2 übermittelt. Die Übermittlung der Fehlermeldung kann über Telefon oder eine Datenleitung erfolgen.

35

- In dem anschließenden Schritt S2 wird in Folge der empfangenen Fehlermeldung von der zweiten Einrichtung 2 über eine geeignete Datenübertragungseinrichtung 3 eine Anfrage auf Anmeldung eines Zugriffs der zweiten Einrichtung 2 auf in der ersten Einrichtung 1 gespeicherte sensible Daten 4 an die erste Einrichtung 1 übermittelt. Die Übermittlung der Anfrage auf Anmeldung eines Zugriffs erfolgt in diesem Ausführungsbeispiel erst nach einer Überprüfung der Fehlermeldung durch einen Benutzer 6 der zweiten Einrichtung 2.
- 10 In Schritt S3 wird die Anfrage auf Anmeldung eines Zugriffs durch die erste Einrichtung 1 an einen ersten Benutzer 5 der ersten Einrichtung 1 ausgegeben.
- 15 Nach Ausgabe der Anfrage an den ersten Benutzer 5 erfolgt (im Belieben des ersten Benutzers 5) in Schritt S4 die Anmeldung des Zugriffs der zweiten Einrichtung 2 auf in der ersten Einrichtung 1 gespeicherte sensible Daten 4 durch den ersten Benutzer 5 der ersten Einrichtung 1. Diese Anmeldung wird über
- 20 die Datenübertragungseinrichtung 3 an die zweite Einrichtung 2 übertragen.
- Daran anschließend wird in Schritt S5 eine erste eindeutige Identifizierung des ersten Nutzers 5 durch die erste Einrichtung 1 abgefragt und über die Datenübertragungseinrichtung 3 an die zweite Einrichtung 2 zur Ausgabe an den zweiten Benutzer 6, 6', 6'' übermittelt.
- 25
- Gleichzeitig wird im parallelen Schritt S6 eine zweite eindeutige Identifizierung eines zweiten Benutzers 6, 6', 6'' der zweiten Einrichtung 2 durch die zweite Einrichtung 2 abgefragt und an die erste Einrichtung 1 zur Ausgabe an den ersten Nutzer 5 übermittelt.
- 30
- Es ist offensichtlich, dass die Schritte S5 und S6 alternative auch sequenziell durchgeführt werden können, wobei wahl-
- 35

weise der Schritt S6 auf den Schritt S5 oder der Schritt S5 auf den Schritt S6 erfolgt.

5 In dem sich an die Schritte S5 und S6 anschließenden Schritt S7 wird die durch die Abfragen gewonnene Konstellation des ersten und zweiten Benutzers 5, 6, 6', 6'' anhand einer vorgegebenen Zuordnungsdatei 7 überprüft, wobei die Zuordnungsdatei 7 jedem ersten Benutzer 5 einen oder mehrere erlaubte zweite Benutzer 6, 6', 6'' zuordnet.

10

Anschließend wird entschieden, ob die durch die Abfragen gewonnene Konstellation erlaubt ist.

15 Ist dies nicht der Fall, wird in Schritt S9 das Ergebnis der Überprüfung an die erste und/oder zweite Einrichtung 1, 2 übertragen und an den jeweiligen ersten und/oder zweiten Nutzer 5, 6', 6'' ausgegeben. Weiter wird der Zugriff der zweiten Einrichtung 2 auf die in der ersten Einrichtung 1 gespeicherten sensiblen Daten 4 unterbunden.

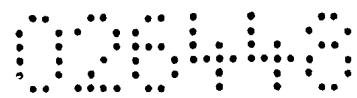
20

Ergibt die Überprüfung, dass die Konstellation erlaubt ist, wird anschließend geprüft, ob in Schritt S4 ein Zugriff der zweiten Einrichtung 2 auf in der ersten Einrichtung 1 gespeicherte sensible Daten 4 angemeldet worden ist.

25

Ist dies der Fall, wird in dem sich anschließenden Schritt S8 das Ergebnis der Überprüfungen an die erste und/oder zweite Einrichtung 1, 2 übertragen und dort an den jeweiligen ersten und/oder zweiten Benutzer 5, 6, 6', 6'' ausgegeben. Weiter
30 wird der Zugriff der zweiten Einrichtung 2 auf die in der ersten Einrichtung 1 gespeicherten sensiblen Daten 4 freigegeben.

35 Wurde jedoch in Schritt S4 kein Zugriff angemeldet, so fährt das Verfahren mit dem vorstehend beschriebenen Schritt S9 fort.



In dem sich an die Schritt S8 und S9 anschließenden Schritt S10 werden die zwischen der ersten und zweiten Einrichtung 1, 2 übertragenen Daten automatisch protokolliert und das so erstellte Protokoll an die ersten und zweiten Einrichtungen 1 und 2 ausgegeben.

Hierauf endet das erfindungsgemäße Verfahren.

Es ist für den Fachmann offensichtlich, dass die Überprüfung, ob ein Zugriff in Schritt S4 angemeldet wurde, anders als in Figur 3 gezeigt bereits unmittelbar nach dem Schritt S4 und damit vor den Schritten S5 und S6 erfolgen kann. In diesem Falle wird mit den Schritten S5 und S6 fortgefahren, wenn in Schritt S4 ein Zugriff angemeldet wurde. Anderenfalls fährt das Verfahren mit Schritt S9 fort.

Die Abfrage einer eindeutigen Identifizierung eines Benutzers 5, 6 umfasst vorzugsweise die Abfrage eines individuellen Passworts und/oder eines biometrischen Merkmals und/oder einer elektronischen Signatur und/oder eines individuellen maschinenlesbaren Gegenstandes.

Die Überprüfung der durch die Abfrage gewonnen Konstellation des ersten und zweiten Nutzers 5, 6 erfolgt vorzugsweise durch die ersten Einrichtung 1 und/oder durch die zweite Einrichtung 2 und/oder durch eine oder mehrere mit der ersten und zweiten Einrichtung 1, 2 verbundene weiteren Einrichtung 8, 8', wobei die Zuordnungsdatei 7 in der bzw. den jeweiligen Einrichtungen 1, 2, 8, 8' gespeichert ist.

Ergibt die Überprüfung der Konstellation des ersten und zweiten Nutzers 5, 6, 6', 6'', dass eine derartige Konstellation in der Zuordnungsdatei 7 nicht als erlaubt gespeichert ist, weist das erfindungsgemäße Verfahren gemäß einem weiteren, in der Figur 3 nicht gezeigten Ausführungsbeispiels ferner den Schritt der Übermittlung eines Genehmigungsformulars von der zweiten Einrichtung 2 an die erste Einrichtung 1 auf. Ein

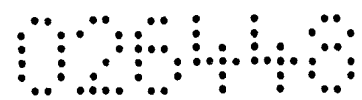
solches Genehmigungsformular kann auch gesendet werden, wenn eine Weitergabe der sensiblen Daten 4 durch den zweiten Benutzer 6, 6', 6'' an einen Dritten erforderlich ist.

- 5 Besonders vorteilhaft ist es, wenn die zweite Einrichtung 2 ein Wartungssystem zur Fernwartung der ersten Einrichtung 1 ist.

- 10 Dabei ist besonders vorteilhaft, wenn die erste Einrichtung 1 ein medizinisches System und die zweite Einrichtung 2 ein Wartungssystem zur Fernwartung des medizinischen Systems ist. In diesem Falle handelt es sich bei den sensiblen Daten 4 um in den medizinischen System gespeicherte Patienten.

Patentansprüche

1. Verfahren zur Steuerung des Zugriffs auf in einer ersten Einrichtung (1) gespeicherte sensible Daten (4) durch eine
5 mit der ersten Einrichtung (1) verbundene zweite Einrichtung (2), aufweisend die folgenden Schritte:
 - (S4) Anmeldung eines Zugriffs der zweiten Einrichtung (2) auf in der ersten Einrichtung (1) gespeicherte sensible Daten (4);
 - 10 - (S5) Abfrage einer ersten eindeutigen Identifizierung des ersten Benutzers (5) durch die erste Einrichtung (1); und
 - (S6) Abfrage einer zweiten eindeutigen Identifizierung eines zweiten Benutzers (6) der zweiten Einrichtung (2) durch die zweite Einrichtung (2);
 - 15 dadurch gekennzeichnet,
dass der Schritt der Anmeldung eines Zugriffs (S4) der zweiten Einrichtung (2) auf in der ersten Einrichtung (1) gespeicherte sensible Daten (4) durch einen ersten Benutzer (5) der ersten Einrichtung (1) erfolgt und eine Übermittlung der An-
20 meldung an die zweite Einrichtung (2) beinhaltet
und dass das Verfahren ferner die folgenden Schritte aufweist:
 - (S7) Überprüfung der durch die Abfragen gewonnenen Konstellation des ersten und zweiten Benutzers (5, 6) anhand einer
25 vorgegebenen Zuordnungsdatei (7), wobei die Zuordnungsdatei (7) jedem ersten Benutzer (5) einen oder mehrere erlaubte zweite Benutzer (6, 6', 6'') zuordnet;
 - (S8) Freischaltung des Zugriffs der zweiten Einrichtung (2) auf in der ersten Einrichtung (1) gespeicherte sensible Daten (4), wenn die Überprüfung der Zuordnung eine erlaubte
30 Konstellation von erstem und zweitem Benutzer (5, 6) feststellt; und
 - (S9) Unterbindung des Zugriffs der zweiten Einrichtung (2) auf in der ersten Einrichtung (1) gespeicherte sensible Daten (4), wenn die Überprüfung der Zuordnung keine erlaubte
35 Konstellation von erstem und zweitem Benutzer (5, 6) feststellt oder ein Zugriff der zweiten Einrichtung (2) auf in



der ersten Einrichtung (1) gespeicherte sensible Daten (4) durch den ersten Benutzer (5) nicht angemeldet wurde.

2. Verfahren nach Anspruch 1,

- 5 d a d u r c h g e k e n n z e i c h n e t,
dass dem Schritt (S4) der Anmeldung eines Zugriffs der zweiten Einrichtung (2) auf in der ersten Einrichtung (1) gespeicherte sensible Daten (4) durch den ersten Benutzer (5) die folgenden Schritte vorausgehen:
- 10 - (S2) Übermittlung einer Anfrage auf Anmeldung eines Zugriffs der zweiten Einrichtung (2) auf in der ersten Einrichtung (1) gespeicherte sensible Daten (4) von der zweiten Einrichtung (2) an die erste Einrichtung (1); und
- (S3) Ausgabe der Anfrage durch die erste Einrichtung (1) an
15 den ersten Benutzer (5) der ersten Einrichtung (1).

3. Verfahren nach Anspruch 2,

- d a d u r c h g e k e n n z e i c h n e t,
dass der Schritt (S2) der Übermittlung einer Anfrage auf Anmeldung eines Zugriffs der zweiten Einrichtung (2) auf in der
20 ersten Einrichtung (1) gespeicherte sensible Daten (4) durch die zweite Einrichtung (2) erst nach Erhalt (S1) einer von der ersten Einrichtung (1) erzeugten und an die zweite Einrichtung (2) übermittelten Mitteilung erfolgt.

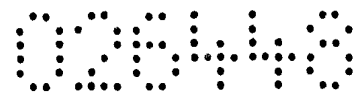
25

4. Verfahren nach Anspruch 3,

- d a d u r c h g e k e n n z e i c h n e t,
dass die von der ersten Einrichtung (1) an die zweite Einrichtung (2) übermittelte Mitteilung eine automatisch erzeugte und/oder übermittelte Fehlermeldung ist.
30

5. Verfahren nach Anspruch 3 oder 4,

- d a d u r c h g e k e n n z e i c h n e t,
dass der Schritt (S2) der Übermittlung einer Anfrage auf Anmeldung eines Zugriffs der zweiten Einrichtung (2) auf in der
35 ersten Einrichtung (1) gespeicherte sensible Daten (4) durch die zweite Einrichtung (2) erst nach einer Überprüfung der



Mitteilung durch den Benutzer (6) der zweiten Einrichtung (2) erfolgt.

6. Verfahren nach einem der vorangegangenen Ansprüche,
5 d a d u r c h g e k e n n z e i c h n e t,
dass die Abfrage der eindeutigen Identifizierung des zweiten Benutzers (6) der zweiten Einrichtung (2) unter Kontrolle der ersten Einrichtung (1) erfolgt.
- 10 7. Verfahren nach einem der vorangegangenen Ansprüche,
d a d u r c h g e k e n n z e i c h n e t,
dass das Ergebnis der Abfrage (S5) der ersten eindeutigen Identifizierung des ersten Benutzers (5) der ersten Einrichtung (1) an die zweite Einrichtung (2) übermittelt und an den
15 zweiten Benutzer (6) ausgegeben wird.
8. Verfahren nach einem der vorangegangenen Ansprüche,
d a d u r c h g e k e n n z e i c h n e t,
dass das Ergebnis der Abfrage (S6) der zweiten eindeutigen
20 Identifizierung des zweiten Benutzers (6) der zweiten Einrichtung (2) an die erste Einrichtung (1) übermittelt und an den ersten Benutzer (5) ausgegeben wird.
9. Verfahren nach einem der vorangegangenen Ansprüche,
25 d a d u r c h g e k e n n z e i c h n e t,
dass die Abfrage einer eindeutigen Identifizierung eines Benutzers (5, 6) die Abfrage eines individuellen Passworts und/oder eines biometrischen Merkmals und/oder einer elektronischen Signatur und/oder eines individuellen maschinenlesbaren Gegenstandes (9) umfasst.
30
10. Verfahren nach einem der vorangegangenen Ansprüche,
d a d u r c h g e k e n n z e i c h n e t,
dass die Überprüfung der durch die Abfrage gewonnenen Konstellation des ersten und zweiten Benutzers (5, 6) durch die
35 erste Einrichtung (1) und/oder durch die zweite Einrichtung (2) und/oder durch eine oder mehrere mit der ersten und

zweiten Einrichtung (1, 2) verbundenen weiteren Einrichtungen (8, 8') erfolgt und die Zuordnungsdatei (7) in der bzw. den jeweiligen Einrichtungen (1, 2, 8, 8') gespeichert ist.

5 11. Verfahren nach einem der vorangegangenen Ansprüche,
d a d u r c h g e k e n n z e i c h n e t,
dass das Ergebnis der Überprüfung der durch die Abfrage ge-
wonnenen Konstellation des ersten und zweiten Benutzers (5,
6) anhand der Zuordnungsdatei (7) an die erste und/oder zwei-
10 te Einrichtung (1, 2) übertragen und an den jeweiligen ersten
und/oder zweiten Benutzer (5, 6) ausgegeben wird.

12. Verfahren nach einem der vorangegangenen Ansprüche,
d a d u r c h g e k e n n z e i c h n e t,
15 dass das Verfahren weiter den folgenden Schritt aufweist:
- (S10) automatische Protokollierung der zwischen der ersten
und der zweite Einrichtung (1, 2) übertragenen Daten und Aus-
gabe des Protokolls an die erste und/oder zweite Einrich-
tung (1, 2).

20 13. Verfahren nach einem der vorangegangenen Ansprüche,
d a d u r c h g e k e n n z e i c h n e t,
dass das Verfahren weiter den folgenden Schritt aufweist:
- Übermittlung eines Genehmigungsformulars an die erste Ein-
25 richtung (1) durch die zweite Einrichtung (2).

14. Verfahren nach einem der vorangegangenen Ansprüche,
d a d u r c h g e k e n n z e i c h n e t,
dass die zweite Einrichtung (2) ein Wartungssystem zur Fern-
30 wartung der ersten Einrichtung (1) ist.

15. Verfahren nach einem der vorangegangenen Ansprüche,
d a d u r c h g e k e n n z e i c h n e t, dass
die erste Einrichtung (1) ein medizinisches System und die
35 zweite Einrichtung (1) ein Wartungssystem zur Fernwartung des
medizinischen Systems ist.

16. Verfahren nach Anspruch 15,
 d a d u r c h g e k e n n z e i c h n e t, dass
 die sensiblen Daten (4) in dem medizinischen System gespei-
 cherte Patientendaten sind.

5

17. Anordnung zur Steuerung des Zugriffs auf in einer ersten
 Einrichtung (1) gespeicherte sensible Daten (4) durch eine
 mit der ersten Einrichtung verbundene zweite Einrichtung (2),
 aufweisend:

10 - eine mit der ersten und zweiten Einrichtung (1, 2) verbun-
 dene Datenübertragungseinrichtung (3) zur Übertragung von Da-
 ten zwischen der ersten Einrichtung (1) und der zweiten Ein-
 richtung (2);

- eine mit der ersten Einrichtung (1) verbundene erste Einga-
 15 beeinrichtung (9) zur Anmeldung eines Zugriffs der zweiten
 Einrichtung (2) auf in der ersten Einrichtung (1) gespeicher-
 te sensible Daten (4) durch einen ersten Benutzer (5) der
 ersten Einrichtung (1);

- eine mit der ersten Einrichtung (1) verbundene erste Abfra-
 20 geeinrichtung (11) zur Abfrage einer ersten eindeutigen Iden-
 tifizierung des ersten Benutzers (5) durch die erste Einrich-
 tung (1); und

- eine mit der zweiten Einrichtung (2) verbundene zweite Ab-
 frageeinrichtung (12) zur Abfrage einer zweiten eindeutigen
 25 Identifizierung eines zweiten Benutzers (6) der zweiten Ein-
 richtung (2) durch die zweite Einrichtung (2);

dadurch gekennzeichnet,
 dass die Anordnung ferner aufweist:

- eine mit der ersten Einrichtung (1) verbundene erste Einga-
 30 beeinrichtung (9) zur Anmeldung eines Zugriffs der zweiten
 Einrichtung (2) auf in der ersten Einrichtung (1) gespeicher-
 te sensible Daten (4) durch einen ersten Benutzer (5) der
 ersten Einrichtung (1); und

- eine mit der ersten und zweiten Einrichtung (1, 2) verbun-
 35 dene Vergleichseinrichtung (15) zur Überprüfung der von der
 ersten und zweiten Abfrageeinrichtung (11, 12) gewonnenen
 Konstellation des ersten und zweiten Benutzers (5, 6) anhand

einer vorgegebenen Zuordnungsdatei (7), wobei die Zuordnungsdatei (7) jedem ersten Benutzer (5) einen oder mehrere erlaubte zweite Benutzer (6, 6', 6'') zuordnet und in der Vergleichseinrichtung (15) gespeichert ist;

5 wobei die erste Einrichtung (1) eine Zugriffssteuerungseinrichtung (13) umfasst, die ausgebildet ist, den Zugriff der zweiten Einrichtung (2) auf in der ersten Einrichtung (1) gespeicherte sensible Daten (4) freizugeben, wenn die Vergleichseinrichtung (15) eine erlaubte Konstellation von erstem und zweitem Benutzer (5, 6) feststellt, und den Zugriff

10 der zweiten Einrichtung (2) auf in der ersten Einrichtung (1) gespeicherte sensible Daten (4) zu unterbinden, wenn die Vergleichseinrichtung (15) keine erlaubte Konstellation von erstem und zweitem Benutzer (5, 6) feststellt oder durch die

15 erste Eingabeeinrichtung (9) kein Zugriff der zweiten Einrichtung (2) auf in der ersten Einrichtung (1) gespeicherte sensible Daten (4) angemeldet wurde.

18. Anordnung nach Anspruch 17,

20 d a d u r c h g e k e n n z e i c h n e t ,
dass die Anordnung ferner aufweist:

- eine mit der ersten Einrichtung (1) verbundene Fehlerkontrolleinrichtung (14) zur automatischen Erzeugung und Übermittlung von Fehlermeldungen an die zweite Einrichtung (2)

25 über die Datenübertragungseinrichtung (3);

- eine mit der zweiten Einrichtung (2) verbundene zweite Ausgabeeinrichtung (17) zur Ausgabe einer von der ersten Einrichtung (1) empfangenen Fehlermeldung an den zweiten Benutzer (6) der zweiten Einrichtung;

30 - eine zweite Eingabeeinrichtung (10) zur Übermittlung einer Anfrage auf Anmeldung eines Zugriffs der zweiten Einrichtung (2) auf in der ersten Einrichtung (1) gespeicherte sensible Daten (4) nach Erhalt einer von der ersten Einrichtung (1) an die zweite Einrichtung (2) übermittelten Fehler-

35 meldung; und

- eine mit der ersten Einrichtung (1) verbundene erste Ausgabe-
beeinrichtung (16) zur Ausgabe der Anfrage an den ersten Be-
nutzer (5) der ersten Einrichtung (1).

5 19. Anordnung nach einem der Ansprüche 17 oder 18,
d a d u r c h g e k e n n z e i c h n e t,
dass die erste Abfrageeinrichtung (11) ausgebildet ist, um
das Ergebnis der Abfrage der ersten eindeutigen Identifizie-
10 rung des ersten Benutzers (5) der ersten Einrichtung (1) über
die Datenübertragungseinrichtung (3) an die zweite Einrich-
tung (2) zu übermitteln, und
dass die zweite Ausgabebeeinrichtung (17) ausgebildet ist, um
das Ergebnis der Abfrage an den zweiten Benutzer (6) aus-
zugeben.

15 20. Anordnung nach einem der Ansprüche 17, 18 oder 19,
d a d u r c h g e k e n n z e i c h n e t,
dass die zweite Abfrageeinrichtung (12) ausgebildet ist, um
das Ergebnis der Abfrage der zweiten eindeutigen Identifizie-
20 rung des zweiten Benutzers (6) der zweite Einrichtung (2) ü-
ber die Datenübertragungseinrichtung (3) an die erste Ein-
richtung (1) zu übermitteln, und
dass die erste Ausgabebeeinrichtung (16) ausgebildet ist, um
das Ergebnis der Abfrage an den ersten Benutzer (5) aus-
25 zugeben.

21. Anordnung nach einem der Ansprüche 17 bis 20,
d a d u r c h g e k e n n z e i c h n e t,
dass die erste Abfrageeinrichtung (11) und die zweite Abfra-
30 geeinrichtung (12) ausgebildet sind, um ein individuelles
Passwort und/oder ein biometrisches Merkmal und/oder eine e-
lektronische Signatur und/oder einen individuellen maschinen-
lesbaren Gegenstand abzufragen.

35 22. Anordnung nach einem der Ansprüche 17 bis 21,
d a d u r c h g e k e n n z e i c h n e t,

dass die Vergleichseinrichtung (15) in der ersten Einrichtung (1) und/oder in der zweiten Einrichtung (2) und/oder durch in einer oder mehreren mit der ersten und zweiten Einrichtung (1, 2) verbundenen weiteren Einrichtungen (8, 8') angeordnet ist.

23. Anordnung nach einem der Ansprüche 17 bis 22, dadurch gekennzeichnet, dass die Vergleichseinrichtung (15) ferner ausgebildet ist, das Vergleichsergebnis über die Datenübertragungseinrichtung (3) an die erste und/oder zweite Einrichtung (1, 2) zu übertragen, dass die erste Ausgabeeinrichtung (16) ausgebildet ist, um das von der Vergleichseinrichtung (15) gewonnene Vergleichsergebnis an den ersten Benutzer (5) auszugeben, und dass die zweite Ausgabeeinrichtung (17) ausgebildet ist, um das von der Vergleichseinrichtung (15) gewonnene Vergleichsergebnis an den zweiten Benutzer (6) auszugeben.

24. Anordnung nach einem der Ansprüche 17 bis 23, dadurch gekennzeichnet, dass die Anordnung ferner eine Protokolliereinrichtung (18) aufweist, um automatisch ein Protokoll der zwischen der ersten und der zweiten Einrichtung (1, 2) übertragenen Daten zu erstellen und das Protokoll über die Datenübertragungseinrichtung (3) an die erste und/oder zweite Einrichtung (1, 2) zu übermitteln.

25. Anordnung nach einem der Ansprüche 17 bis 24, dadurch gekennzeichnet, dass die zweite Einrichtung (2) ferner ausgebildet ist, über die Datenübertragungseinrichtung (3) ein Genehmigungsformular an die erste Einrichtung (1) zu übertragen.

26. Anordnung nach einem der Ansprüche 17 bis 25, dadurch gekennzeichnet,

dass die zweite Einrichtung (2) ein Wartungssystem zur Fernwartung der ersten Einrichtung (1) ist.

27. Anordnung nach einem der Ansprüche 17 bis 26,
5 d a d u r c h g e k e n n z e i c h n e t, dass
die erste Einrichtung (1) ein medizinisches System und die
zweite Einrichtung (1) ein Wartungssystem zur Fernwartung des
medizinischen Systems ist.
- 10 28. Anordnung nach Anspruch 27,
d a d u r c h g e k e n n z e i c h n e t, dass
die sensiblen Daten (4) in dem medizinischen System gespeichert
Patientendaten sind.

FIG 1

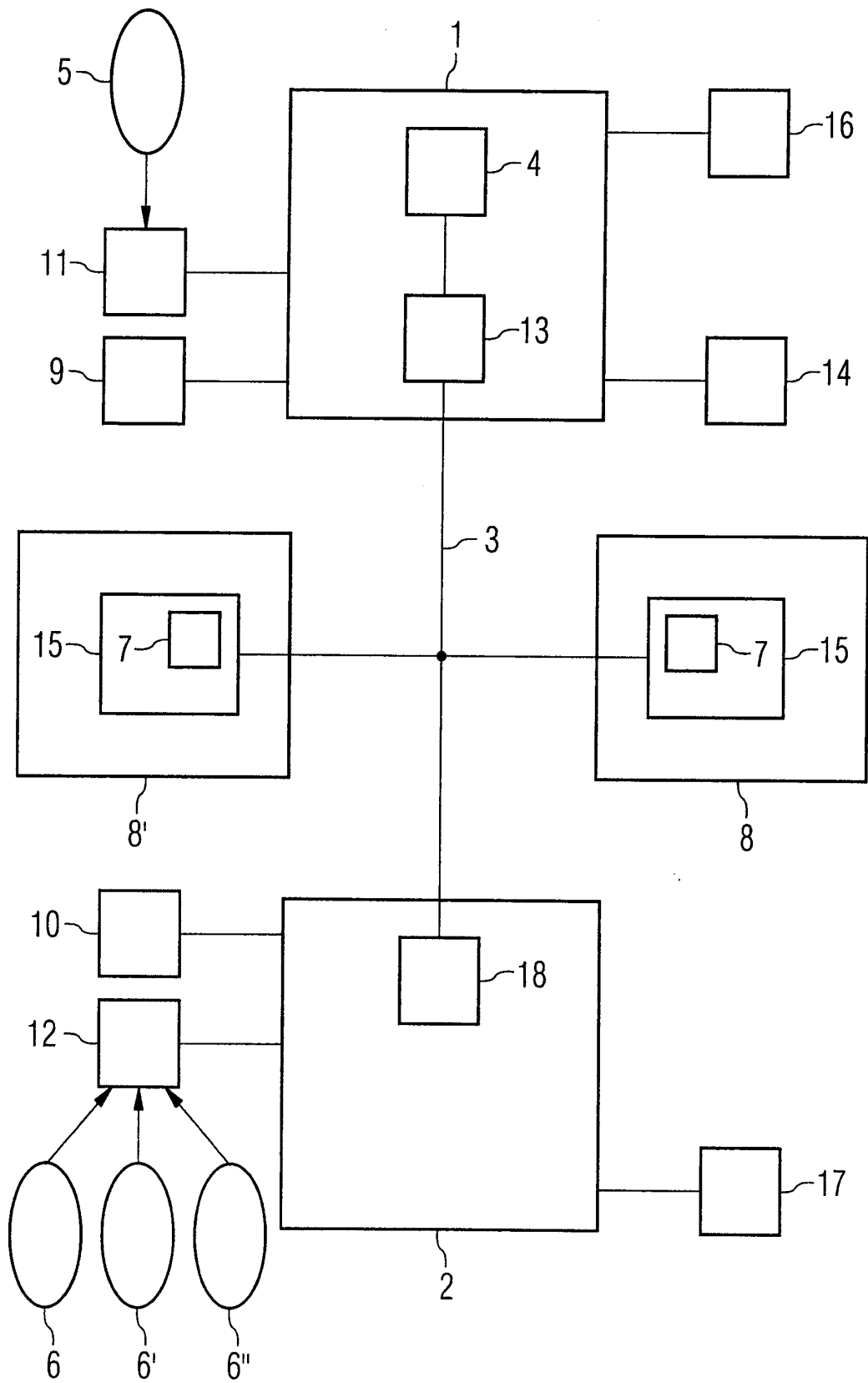


FIG 2

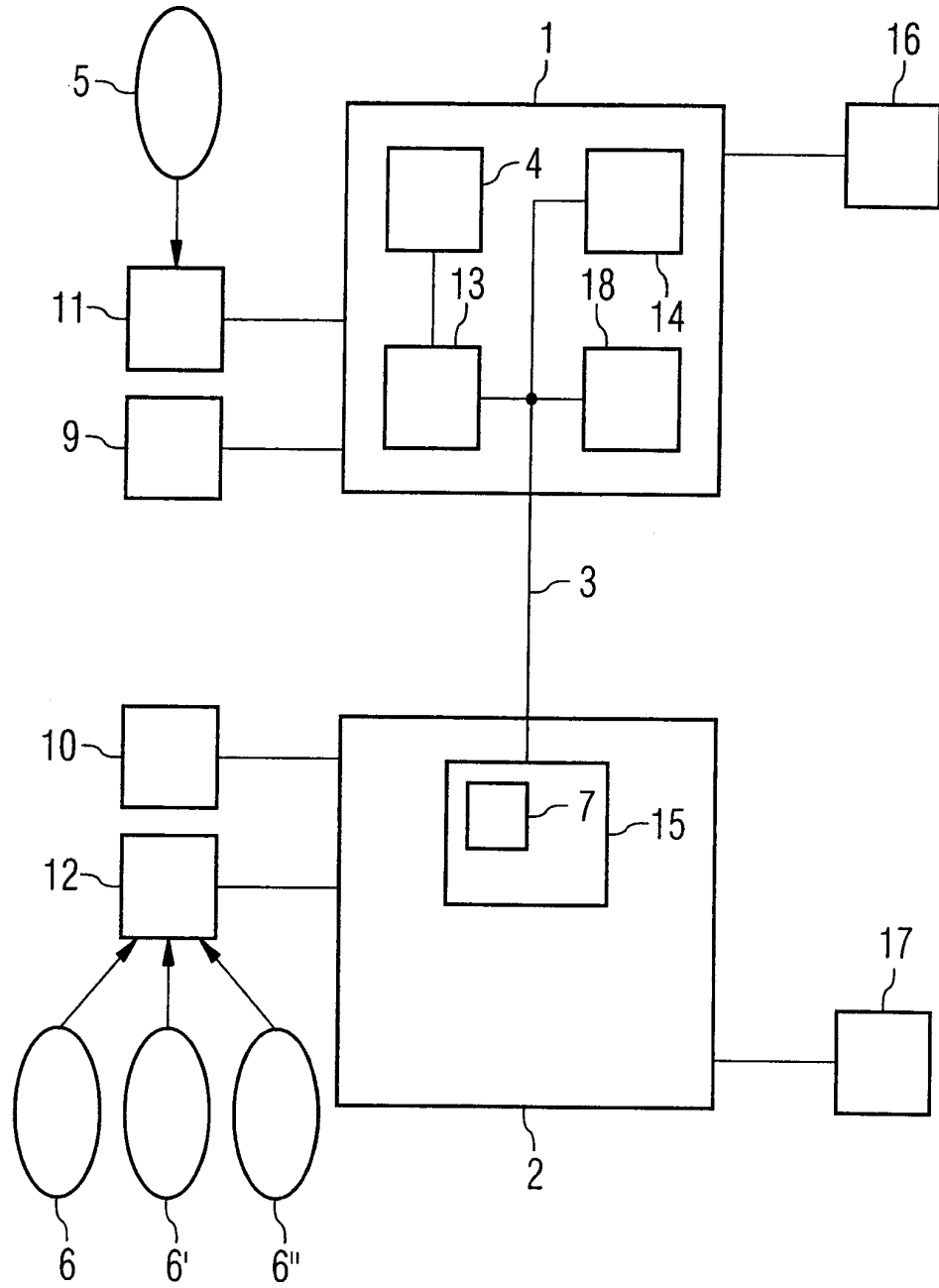


FIG 3

