(19) Deutsches Patent- und Markenamt

(10) **DE 10 2018 103 399 A1** 2018.08.23

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2018 103 399.0**
(22) Anmeldetag: **15.02.2018**
(43) Offenlegungstag: **23.08.2018**

(51) Int Cl.: ***G06F 21/33*** (2013.01)
G06F 21/44 (2013.01)
G06F 21/64 (2013.01)

(30) Unionspriorität:
2017-028424 17.02.2017 JP

(71) Anmelder:
Canon Kabushiki Kaisha, Tokyo, JP

(74) Vertreter:
TBK, 80336 München, DE

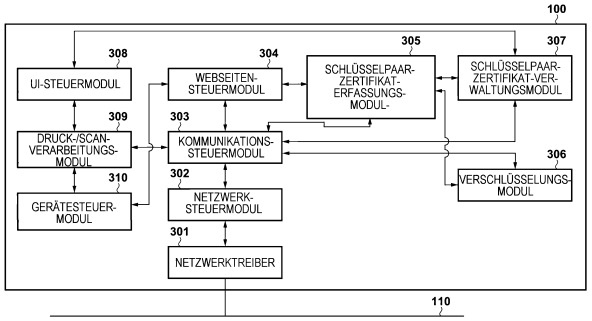
(72) Erfinder:
Kakutani, Naoya, Tokyo, JP; Yamauchi, Hisayuki, Tokyo, JP

Prüfungsantrag gemäß § 44 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **INFORMATIONSVERARBEITUNGSVORRICHTUNG, BILDERZEUGUNGSVORRICHTUNG, SYSTEM, VERFAHREN ZUR STEUERUNG DERSELBEN UND SPEICHERMEDIUM**

(57) Zusammenfassung: Eine Informationsverarbeitungsvorrichtung erzeugt ein öffentliches Schlüsselpaar gemäß einer Zertifikatsausstellungsanforderung, erzeugt eine Zertifikatssignierungsanforderung basierend auf dem öffentlichen Schlüsselpaar und überträgt die Zertifikatssignierungsanforderung an eine externe Vorrichtung. Die Informationsverarbeitungsvorrichtung erfasst ein elektronisches Zertifikat und ein Zertifikatsausstellungsanforderungsergebnis von der externen Vorrichtung als Antwort auf die Ausstellungsanforderung und stellt die Anwendung des erfassten elektronischen Zertifikats ein.



Beschreibung

HINTERGRUND DER ERFINDUNG

Gebiet der Erfindung

[0001] Die vorliegende Erfindung bezieht sich auf eine Informationsverarbeitungsvorrichtung, eine Bilderzeugungsvorrichtung, ein System, ein Verfahren zur Steuerung derselben und ein Speichermedium.

Beschreibung der verwandten Technik

[0002] Bei Kommunikation mit einem externen Server verwendet ein Personalcomputer (PC), der sich mit einem Netzwerk verbindet, wie etwa demjenigen eines Büros und eines mobilen Geräts, das einer Einzelperson gehört, ein Öffentlicher-Schlüssel-Zertifikat (z.B. ein digitales Zertifikat), um gesicherte bzw. geschützte Kommunikation und Authentisierung durchzuführen.

[0003] Nicht nur, dass ein Multifunktionsperipheriegerät Bilder einfach druckt und überträgt, sondern hat es in den letzten Jahren auch eine Funktion zur Bereitstellung eines Dateispeicherdiensts für einen PC, indem Bilddaten in dem Multifunktionsperipheriegerät gespeichert werden. Daher ist es dazu gekommen, dass ein Multifunktionsperipheriegerät die Rolle einer Informationsverarbeitungsvorrichtung ausübt, ähnlich zu derjenigen von anderen Servervorrichtungen, die in einem Netzwerk vorhanden sind. Um eine sichere und gesicherte bzw. geschützte Büroumgebung zu unterhalten, während diese Informationsverarbeitungsvorrichtungen in einem Netzwerk verwendet werden, ist Kommunikation basierend auf einer Authentisierung unter Verwendung eines elektronischen Zertifikats (d.h. eines digitalen Zertifikats) erforderlich. Im Allgemeinen wurde sicherere Netzwerkidentifikation und Authentisierung durch Verwendung der Technik basierend auf Public-Key-Infrastruktur (PKI) implementiert, die ein solches elektronisches Zertifikat verwendet (siehe RFC3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certificate Practices Framework).

[0004] Zum Beispiel, wenn eine Informationsverarbeitungsvorrichtung ein Client sein soll, kann die Authentizität eines Servers verifiziert werden, indem ein Öffentlicher-Schlüssel-Zertifikat des Servers von dem Server und ein Zertifizierungsstelle-(CA-)Zertifikat, das bei Ausstellung des Öffentlicher-Schlüssel-Zertifikats des Servers verwendet wurde, erhalten bzw. erfasst werden. Auch ist es für den Server möglich, die Authentizität des Clients zu verifizieren, indem ein Öffentlicher-Schlüssel-Zertifikat des Clients von dem Client (z.B. der Informationsverarbeitungsvorrichtung) an den Server bereitgestellt wird. Zusätzlich kann, wenn die Informationsverarbeitungsvorrichtung als der Server agieren soll, ein Öffentlicher-Schlüssel-Zertifikat des Servers von der Informationsverarbeitungsvorrichtung an einen Client verbreitet werden, der zu verbinden ist, sodass der Client die Authentizität der Informationsverarbeitungsvorrichtung als der Server verifizieren kann. Auf diese Art und Weise wurde ein elektronisches Zertifikat als ein wichtiges Werkzeug für Informationsverarbeitungsvorrichtungen zur Durchführung einer Authentisierung/Verifikation und einer Identifikation in einer Netzwerkkommunikation/-umgebung verwendet. Zum Beispiel sind SSL, TLS, IEE-E802.1X und IPSEC einige der Kommunikationsprotokolle, die in einer solchen gesicherten bzw. geschützten Kommunikation basierend auf einem elektronischen Zertifikat verwendet werden.

[0005] Da ein elektronisches Zertifikat in einer Informationsverarbeitungsvorrichtung gespeichert/gehalten werden muss, wird herkömmlich ein elektronisches Zertifikat, das durch eine Zertifizierungsstelle ausgestellt wurde, manuell in einem Speicher der Informationsverarbeitungsvorrichtung gespeichert, wobei ein Benutzer der Informationsverarbeitungsvorrichtung die Speicherung manuell durchführt. Dieses Speicherverfahren wird durchgeführt durch Herunterladen des elektronischen Zertifikats von der Zertifizierungsstelle, die das elektronische Zertifikat ausstellt, Kopieren des elektronischen Zertifikats von einem externen Speicher wie etwa einem USB-Speicher, oder Kopieren des elektronischen Zertifikats, das per Email empfangen wurde, in einen vorbestimmten Ordner in dem Speicher.

[0006] Abhängig von der tatsächlichen Implementierung der Kommunikation kann ein separates elektronisches Zertifikat für jede Informationsverarbeitungsvorrichtung verwendet werden. Zum Beispiel wird im Allgemeinen, wenn IEEE802.1X oder dergleichen für die Kommunikation eingesetzt wird, ein elektronisches Zertifikat für jede Informationsverarbeitungsvorrichtung individuell gespeichert, um eine Client-Authentisierung durchzuführen. Auch hat ein elektronisches Zertifikat eine Gültigkeitsdauer bzw. Laufzeit (d.h. einen Zeitraum oder ein/eine Datum/Zeit, nach dem/der das elektronische Zertifikat nicht mehr gültig bzw. nicht mehr zur Authentisierung/Verifikation nutzbar ist), und wird eine Kommunikation unter Verwendung des elektronischen Zertifikats gesperrt bzw. blockiert, wenn die Gültigkeitsdauer bzw. Laufzeit abläuft. Daher muss ein elektronisches Zertifikat, das in einer Vorrichtung (wie etwa der Informationsverarbeitungsvorrichtung) gespeichert ist, aktualisiert werden, wenn die Gültigkeitsdauer bzw. Laufzeit abläuft, oder (bevorzugt unmittelbar) vor dem Ablauf. Wenn ein elektronisches Zertifikat zu verwenden ist, ist es außerdem notwendig, jedes elektronische Zertifikat, das in Entsprechung zu jeder Kommunikationsanwendung zu verwenden sein wird, wie etwa TLS oder IEEE802.1X, die durch jede Informationsverar-

beitungsvorrichtung zu verwenden sein wird, manuell einzustellen.

[0007] In einem Fall, in dem es viele Informationsverarbeitungsvorrichtungen gibt, die elektronische Zertifikate handhaben/benötigen, kann jedoch, wenn ein Benutzer jedes elektronische Zertifikat für jede dieser Informationsverarbeitungsvorrichtungen manuell hinzuzufügen, zu aktualisieren und einzustellen hat, dies eine große Arbeitsbelastung bzw. Last auf den Benutzer ausüben und zu viel Zeit benötigen.

KURZFASSUNG DER ERFINDUNG

[0008] Ein Aspekt der vorliegenden Erfindung besteht darin, eine nachteilige Wirkung, die sich aus dem vorstehend dargelegten Problem mit der herkömmlichen Technik ergibt, zu beseitigen bzw. zu vermeiden oder zumindest zu vermindern.

[0009] Ein Merkmal der vorliegenden Erfindung besteht darin, eine Technik bzw. einen Mechanismus bereitzustellen, um ein elektronisches Zertifikat in einer Informationsverarbeitungsvorrichtung einfach hinzuzufügen und zu aktualisieren.

[0010] Gemäß einem ersten Aspekt der vorliegenden Erfindung ist eine Informationsverarbeitungsvorrichtung bereitgestellt, mit: einem Erzeuger, der konfiguriert ist zum Erzeugen eines öffentlichen Schlüsselpaars und Erzeugen einer Zertifikatssignierungsanforderung basierend auf dem erzeugten öffentlichen Schlüsselpaar; einem Sender, der konfiguriert ist zum Übertragen einer Elektronisches-Zertifikat-Ausstellungsanforderung, die die erzeugte Zertifikatssignierungsanforderung umfasst, an eine externe Vorrichtung; einem Empfänger, der konfiguriert ist zum Empfangen einer Antwort, die von der externen Vorrichtung als Antwort auf die Elektronisches-Zertifikat-Ausstellungsanforderung übertragen wird; einer ersten Erfassungseinheit, die konfiguriert ist zum Erfassen eines elektronischen Zertifikats, das in der durch den Empfänger empfangenen Antwort umfasst ist; und einem Prozessor, der konfiguriert ist zum Bewirken, dass eine Anwendung ihre Verwendung des elektronischen Zertifikats ermöglicht, das durch die erste Erfassungseinheit erfasst wird.

[0011] Gemäß einem zweiten Aspekt der vorliegenden Erfindung ist ein Verfahren zur Steuerung einer Informationsverarbeitungsvorrichtung bereitgestellt, die konfiguriert ist zum Durchführen einer Kommunikation unter Verwendung eines elektronischen Zertifikats, wobei das Verfahren aufweist: Erzeugen eines öffentlichen Schlüsselpaars und Erzeugen einer Zertifikatssignierungsanforderung basierend auf dem erzeugten öffentlichen Schlüsselpaar; Übertragen einer Elektronisches-Zertifikat-Ausstellungsanforderung, die die erzeugte Zertifikatssignierungsanforderung umfasst, an eine externe Vorrichtung; Empfangen einer Antwort, die von der externen Vorrichtung als Antwort auf die Elektronisches-Zertifikat-Ausstellungsanforderung übertragen wird; Erfassen eines elektronischen Zertifikats, das in der beim Empfangen empfangenen Antwort umfasst ist; und Bewirken, dass eine Anwendung ihre Verwendung des elektronischen Zertifikats ermöglicht, das beim Erfassen erfasst wird.

[0012] Gemäß einem dritten Aspekt der vorliegenden Erfindung ist eine Bilderzeugungsvorrichtung bereitgestellt, mit: einer Verwaltungseinheit, die konfiguriert ist zum Verwalten eines elektronischen Zertifikats; einer Aktualisierungsverwaltungseinheit, die konfiguriert ist zum Einstellen einer aus einer Vielzahl von Aktualisierungsregeln ausgewählten Aktualisierungsregel, die für das durch die Verwaltungseinheit verwaltete elektronische Zertifikat anwendbar ist; und einem Sender, der konfiguriert ist zum Übertragen, basierend auf der eingestellten Aktualisierungsregel, einer Elektronisches-Zertifikat-Aktualisierungsanforderung an eine externe Vorrichtung.

[0013] Gemäß einem vierten Aspekt der vorliegenden Erfindung ist ein Verfahren zur Steuerung einer Bilderzeugungsvorrichtung bereitgestellt, die konfiguriert ist zum Durchführen einer Kommunikation unter Verwendung eines elektronischen Zertifikats, wobei das Verfahren aufweist: Verwalten des elektronischen Zertifikats; Einstellen einer aus einer Vielzahl von Aktualisierungsregeln ausgewählten Aktualisierungsregel, die für das verwaltete elektronische Zertifikat anwendbar ist; und Übertragen, basierend auf der eingestellten Aktualisierungsregel, einer Elektronisches-Zertifikat-Aktualisierungsanforderung an eine externe Vorrichtung.

[0014] Gemäß einem fünften Aspekt der vorliegenden Erfindung ist ein System bereitgestellt, mit zumindest einer Informationsverarbeitungsvorrichtung gemäß einem der Ansprüche 1 bis 9 und einer externen Vorrichtung, die aufweist: einen Empfänger, der konfiguriert ist zum Empfangen der durch die Informationsverarbeitungsvorrichtung übertragenen Elektronisches-Zertifikat-Ausstellungsanforderung; einen Prozessor, der konfiguriert ist zum Verarbeiten der empfangenen Elektronisches-Zertifikat-Ausstellungsanforderung, Erfassen eines elektronischen Zertifikats und Erzeugen einer Antwort, die das erfasste elektronische Zertifikat umfasst; und einen Sender, der konfiguriert ist zum Übertragen der erzeugten Antwort an die Informationsverarbeitungsvorrichtung.

[0015] Gemäß einem sechsten Aspekt der vorliegenden Erfindung ist ein Verfahren zur Steuerung eines Systems bereitgestellt, das eine externe Vorrichtung und zumindest eine Informationsverarbeitungsvorrichtung aufweist, die konfiguriert ist zum Durchführen einer Kommunikation unter Verwen-

dung eines elektronischen Zertifikats, wobei das Verfahren aufweist: das Verfahren zur Steuerung einer Informationsverarbeitungsvorrichtung gemäß einem der Ansprüche 10 bis 17 und an der externen Vorrichtung: Empfangen der durch die Informationsverarbeitungsvorrichtung übertragenen Elektronisches-Zertifikat-Ausstellungsanforderung; Verarbeiten der empfangenen Elektronisches-Zertifikat-Ausstellungsanforderung, Erfassen eines elektronischen Zertifikats und Erzeugen einer Antwort, die das erfasste elektronische Zertifikat umfasst; und Übertragen der erzeugten Antwort an die Informationsverarbeitungsvorrichtung.

[0016] Weitere Merkmale, Aspekte und Vorteile der vorliegenden Erfindung werden aus der folgenden Beschreibung von Ausführungsbeispielen unter Bezugnahme auf die beigefügten Zeichnungen deutlich. Jedes der Ausführungsbeispiele der vorliegenden Erfindung, die nachstehend beschrieben sind, kann einzeln oder als Kombination von einer Vielzahl der Ausführungsbeispiele implementiert werden. Auch können Merkmale von unterschiedlichen Ausführungsbeispielen kombiniert werden, wenn dies notwendig ist, oder wenn die Kombination von Elementen oder Merkmalen von individuellen Ausführungsbeispielen in einem einzigen Ausführungsbeispiel vorteilhaft ist.

[0017] Die begleitenden Zeichnungen, die in die Schrift eingebunden sind und einen Teil von dieser bilden, veranschaulichen Ausführungsbeispiele der Erfindung, und sie dienen, zusammen mit der Beschreibung, zur Erläuterung der Prinzipien der Erfindung.

Figurenliste

Fig. 1 ist ein Blockschaltbild, das eine Netzwerkanordnung bzw. -ausgestaltung oder ein System gemäß einem ersten Ausführungsbeispiel der vorliegenden Erfindung veranschaulicht;

Fig. 2 ist ein Blockschaltbild, das eine Hardwareanordnung bzw. -ausgestaltung eines Multifunktionsperipheriegeräts gemäß dem ersten Ausführungsbeispiel veranschaulicht;

Fig. 3 ist ein Blockschaltbild, das Softwaremodule veranschaulicht, die in einem Programm umfasst sind, das auf dem Multifunktionsperipheriegerät gemäß dem ersten Ausführungsbeispiel läuft;

Fig. 4A und **Fig. 4B** sind Sequenzdiagramme, die einen Gesamtprozessablauf veranschaulichen, der in einer Netzwerkanordnung oder einem System gemäß dem ersten Ausführungsbeispiel abläuft;

Fig. 5A ist ein Ablaufdiagramm, das eine Verarbeitung zur Erfassung einer Schlüsselpaar/Elektronisches-Zertifikat-Liste und Erzeugung von Anzeigedaten in Schritt S402 von **Fig. 4A** durch das Multifunktionsperipheriegerät gemäß dem ersten Ausführungsbeispiel veranschaulicht;

Fig. 5B ist ein Ablaufdiagramm, das eine Verarbeitung veranschaulicht, die durchgeführt wird, wenn eine von einem PC übertragene Detailinformationsanzeigeanforderung durch das Multifunktionsperipheriegerät gemäß dem ersten Ausführungsbeispiel empfangen wird;

Fig. 6 ist ein Ablaufdiagramm, das einen Verbindungseinrichtungsprozess zur Herstellung einer Verbindung mit einer Zertifizierungs-/Registrierungsstelle in Schritt S407 von **Fig. 4A** veranschaulicht, der durch das Multifunktionsperipheriegerät gemäß dem ersten Ausführungsbeispiel durchgeführt wird;

Fig. 7 ist ein Ablaufdiagramm, das einen Prozess zur Erfassung/Registrierung eines Zertifizierungsstelle-(CA-)Zertifikats in Schritt S412 bis Schritt S416 von **Fig. 4A** veranschaulicht, der durch das Multifunktionsperipheriegerät gemäß dem ersten Ausführungsbeispiel durchgeführt wird;

Fig. 8A und **Fig. 8B** sind Ablaufdiagramme, die einen Prozess einer Zertifikatsausstellungsanforderung/-erfassung in Schritt S419 bis Schritt S424 von **Fig. 4B** veranschaulichen, der durch das Multifunktionsperipheriegerät gemäß dem ersten Ausführungsbeispiel durchgeführt wird;

Fig. 9 ist ein Ablaufdiagramm, das eine Verarbeitung in Bezug auf einen Neustart des Multifunktionsperipheriegeräts in Schritt S424 bis Schritt S427 von **Fig. 4B** veranschaulicht, die durch das Multifunktionsperipheriegerät gemäß dem ersten Ausführungsbeispiel durchgeführt wird;

Fig. 10A-10B, **Fig. 11A-11B**, **Fig. 12A-12B**, **Fig. 13A-13B**, **Fig. 14A-14B** und **Fig. 15** zeigen Bildschirmansichten, die Beispiele eines Webseitenbildschirms von einer Fernbenutzerschnittstelle (RUI) zeigen, die auf einem PC gemäß dem ersten Ausführungsbeispiel angezeigt wird;

Fig. 16 zeigt eine Bildschirmansicht, die ein Beispiel von Detailinformationen des elektronischen Zertifikats zeigt, die auf dem PC gemäß dem ersten Ausführungsbeispiel angezeigt werden;

Fig. 17A bis **Fig. 17C** zeigen konzeptionelle Darstellungen einer Schlüsselpaar/Elektronisches-Zertifikat-Detailinformationen-Datenbank, die durch ein Schlüsselpaar-Zertifikat-Verwaltungsmodul des Multifunktionsperipheriegeräts gemäß dem ersten Ausführungsbeispiel verwaltet wird;

Fig. 18 zeigt eine Darstellung, die ein Beispiel eines Elektronisches-Zertifikat-Aktualisierungsreservierung-Einstellungsbildschirms veranschaulicht, der durch ein Multifunktionsperipheriegerät gemäß einem zweiten Ausführungsbeispiel bereitgestellt wird; und

Fig. 19 ist ein Ablaufdiagramm, das eine Verarbeitung veranschaulicht, die durchgeführt wird, wenn eine automatische Aktualisierungsfunktion eines elektronischen Zertifikats basierend auf der Elektronisches-Zertifikat-Aktualisierungsreservierung-Einstellung ausgeführt/durchgeführt wird, die auf dem Multifunktionsperipheriegerät gemäß dem zweiten Ausführungsbeispiel eingestellt ist.

BESCHREIBUNG DER AUSFÜHRUNGSBEISPIELE

[0018] Ausführungsbeispiele der vorliegenden Erfindung werden hierin nachstehend unter Bezugnahme auf die beiliegenden Zeichnungen ausführlich beschrieben. Es ist selbstverständlich, dass die folgenden Ausführungsbeispiele nicht zur Beschränkung der Ansprüche der vorliegenden Erfindung bestimmt sind, und dass nicht alle der Kombinationen der Aspekte, die gemäß den folgenden Ausführungsbeispielen beschrieben sind, mit Bezug auf die Mittel zur Lösung der Probleme gemäß der vorliegenden Erfindung notwendigerweise erforderlich sind. Es ist zu beachten, dass als ein Beispiel einer Informationsverarbeitungsvorrichtung, die ein elektronisches Zertifikat gemäß den Ausführungsbeispielen verwendet und verwaltet, ein Multifunktionsperipheriegerät (ein digitales Multifunktionsperipheriegerät/MFP) beschrieben wird. Die vorliegende Erfindung ist jedoch nicht auf das Multifunktionsperipheriegerät beschränkt, und die vorliegende Erfindung ist auf jegliche Vorrichtung oder eine Komponente von dieser anwendbar, solange es sich um eine Informationsverarbeitungsvorrichtung handelt, in der ein elektronisches Zertifikat verwendet oder verwaltet werden kann.

[Erstes Ausführungsbeispiel]

[0019] **Fig. 1** ist ein Blockschaltbild zur Erläuterung einer Netzwerkanordnung bzw. -ausgestaltung (oder eines Systems) gemäß dem ersten Ausführungsbeispiel der vorliegenden Erfindung.

[0020] Ein Multifunktionsperipheriegerät **100** mit einer Druckfunktion kann Druckdaten, gescannte Bilddaten, Geräteverwaltungsinformationen und dergleichen mit einer anderen Informationsverarbeitungsvorrichtung über ein Netzwerk **110** austauschen. Das Multifunktionsperipheriegerät **100** ist im Stande, eine verschlüsselte Kommunikation unter Verwendung von Kommunikations-/ Kryptographieprotokollen durchzuführen, wie etwa Transport Layer Security (TLS), Internet Protocol Security (IPSEC) und IEEE802.1X, und hält (z.B. speichert oder verwaltet) ein Öffentlicher-Schlüssel-Paar und ein elektronisches Zertifikat (d.h. ein digitales Zertifikat), die zum Durchführen dieser Verschlüsselungsprozesse verwendet werden. Hier kann das Multifunktionsperipheriegerät 100 ein Beispiel einer Bilderzeugungsvorrichtung sein. Es ist selbstverständliche, dass eine solche Bilderzeugungsvorrichtung nicht auf das Multifunktionsperipheriegerät beschränkt ist und eine Vorrichtung sein kann, die ausschließlich als Faxvorrichtung, Drucker oder Kopierer funktioniert, oder eine Vorrichtung sein kann, die als eine beliebige Kombination dieser Einzelfunktionsvorrichtungen funktioniert. Ein weiteres Multifunktionsperipheriegerät **101** ist ebenfalls mit dem Netzwerk **110** verbunden, und dieses zweite Multifunktionsperipheriegerät **101** kann die gleichen Funktionen wie diejenigen des Multifunktionsperipheriegeräts 100 aufweisen oder zumindest einige von dessen Funktionen teilen. Obgleich nur das Multifunktionsperipheriegerät **100** hierin nachstehend hauptsächlich beschrieben wird, ist es selbstverständlich, dass der Austausch bzw. die Kommunikation von elektronischen Zertifikaten zwischen einer bzw. für eine Vielzahl von Multifunktionsperipheriegeräten durchgeführt werden kann.

[0021] Eine Zertifizierungs-/Registrierungsstelle **102** hat eine Funktion als Zertifizierungsstelle (CA: „Certificate Authority“) zum Ausstellen eines elektronischen Zertifikats und eine Funktion als Registrierungsstelle (RA: „Registration Authority“) zum Entgegennehmen (in einigen Fällen einschließlich einer Verifikation/Authentisierung) einer Elektronisches-Zertifikat-Ausstellungsanforderung und Durchführen eines Registrierungsprozesses basierend auf der entgegengenommenen Anforderung. Das heißt, dass diese Zertifizierungs-/Registrierungsstelle 102 zum Beispiel eine Servervorrichtung (die ein Beispiel einer Informationsverarbeitungsvorrichtung darstellt) ist, die eine Funktion zum Verteilen bzw. Verbreiten eines CA-Zertifikats (z.B. zum Authentisieren einer elektronischen CA-Signatur auf einem Serverzertifikat) und Ausstellen/Registrieren eines elektronischen Zertifikats (z.B. zum Herstellen einer gesicherten bzw. geschützten Kommunikation) über das Netzwerk **110** durchführt. Bei dem ersten Ausführungsbeispiel sei angenommen, dass SCEP (Simple Certificate Enrollment Protocol) als das Kommunikationsprotokoll des Netzwerks **110** verwendet wird. Es ist jedoch selbstverständlich, dass verschiedene andere Typen von Protokollen zum Ausstellen/Verwalten eines elektronischen Zertifikats mit der Netzwerkanordnung bzw. -ausgestaltung des ersten Ausführungsbeispiels ebenfalls verwendet werden können, solange sie in der Lage sind, entsprechende Funktionen bereitzustellen. Eine Informationsverarbeitungsvorrichtung, wie etwa das Multifunktionsperipheriegerät 100, verwendet dieses SCEP zum Kommunizieren mit der Zertifizierungs-/Registrierungsstelle **102** über

das Netzwerk **110**, um eine Elektronisches-Zertifikat-Ausstellungsanforderung zu übertragen und das ausgestellte elektronische Zertifikat zu erhalten bzw. zu erfassen. Das Multifunktionsperipheriegerät 100 gemäß dem ersten Ausführungsbeispiel hat eine Webserverfunktion und kann eine Funktion einer Fernbenutzerschnittstelle (RUI: „Remote User Interface“) im Webseitenformat, die verwendet werden kann, um eine Verarbeitung für die Ausstellungsanforderung und die Erfassung (Erlangung) des elektronischen Zertifikats auszuführen/durchzuführen, auf dem Netzwerk **110** veröffentlichen.

[0022] Wenn eine Elektronisches-Zertifikat-Ausstellungsanforderung von einer Informationsverarbeitungsvorrichtung über das Netzwerk **110** empfangen wird, führt die Zertifizierungs-/Registrierungsstelle **102** eine Verarbeitung zur Ausstellung und Registrierung eines elektronischen Zertifikats basierend auf der empfangenen Ausstellungsanforderung durch, und überträgt sie das ausgestellte elektronische Zertifikat als eine Antwort auf die Ausstellungsanforderung. Es ist zu beachten, dass, obgleich bei diesem ersten Ausführungsbeispiel die Funktion von einer CA und die Funktion von einer RA durch die gleiche Servervorrichtung implementiert werden, die vorliegende Erfindung nicht darauf beschränkt ist. Es ist auch möglich, eine Anordnung bzw. Ausgestaltung anzunehmen, in der die CA und die RA als separate Servervorrichtungen implementiert werden, zum Beispiel als ein CA-Server und ein separater RA-Server. Zusätzlich ist, obgleich das erste Ausführungsbeispiel SCEP als das Protokoll zum Vornehmen einer Elektronisches-Zertifikat-Ausstellungsanforderung und zum Erfassen des ausgestellten elektronischen Zertifikats verwendet, die vorliegende Erfindung nicht darauf beschränkt ist, solange ein Protokoll angenommen wird, das die gleichen oder kompatible Funktionen aufweist. Zum Beispiel ist es möglich, ein Protokoll wie etwa CMP (Certificate Management Protocol) oder EST (Enrollment over Secure Transport) zu verwenden.

[0023] Ein PC **103** ist ein Personalcomputer. Der PC **103** hat eine Webbrowserfunktion. Dies macht es möglich (d.h. ermöglicht es einem Benutzer oder einer Informationsverarbeitungsvorrichtung), HTML-Dokumente und Webseiten zu browsen und zu verwenden, die durch eine Informationsverarbeitungsvorrichtung veröffentlicht wurden, die mit dem Netzwerk **110** verbunden ist. Es ist selbstverständlich, dass, obgleich der PC **103** hierin gezeigt/beschrieben ist, jegliche Vorrichtung bzw. jegliches Gerät, die bzw. das im Stande ist, eine Webbrowserfunktion bereitzustellen oder Informationen anzuzeigen und eine Benutzereingabe anzunehmen (z.B. ein Tablet, ein Mobiltelefon, ein Gerät basierend auf einer tragbaren Technologie, unter anderem), stattdessen verwendet werden kann, solange sie bzw. es mit der Informationsverarbeitungsvorrichtung in dem Netzwerk **110** kommunikationsfähig ist.

[0024] Als Nächstes wird der Überblick der Erfassung eines elektronischen Zertifikats und eines Aktualisierungsprozesses gemäß dem ersten Ausführungsbeispiel beschrieben.

[0025] Ein Administrator des Multifunktionsperipheriegeräts **100** verwendet einen auf dem PC **103** installierten Webbrowser, um eine Verbindung mit einer Webseite für eine Elektronisches-Zertifikat-Ausstellungsanforderung und -Erfassung herzustellen, die durch das Multifunktionsperipheriegerät **100** zugänglich gemacht wird (z.B. indem sie veröffentlicht wird). Der Administrator verwendet die Webseite zum Einstellen von Einstellungen und Anweisungen zum Ausführen der Prozesse für die Elektronisches-Zertifikat-Ausstellungsanforderung und -Erfassung (d.h. die Ausstellungsanforderungs- und Erfassungs-/Erlangungsprozesse des elektronischen Zertifikats). Das Multifunktionsperipheriegerät **100** macht (d.h. erzeugt), gemäß den Einstellungen und den Anweisungen (z.B. Informationen/Inhalten, wie sie über die Webseite angewiesen werden), die durch den Administrator eingestellt werden/sind, eine Erfassungsanforderung (eine Erlangungsanforderung) für ein CA-Zertifikat und eine Elektronisches-Zertifikat-Ausstellungsanforderung an die Zertifizierungs-/Registrierungsstelle **102** mittels SCEP. Das Multifunktionsperipheriegerät **100** erhält bzw. erfasst auch das elektronische Zertifikat, das durch die Zertifizierungs-/Registrierungsstelle **102** ausgestellt wird, da/wie es in der Antwort auf die Elektronisches-Zertifikat-Ausstellungsanforderung umfasst ist. Das Multifunktionsperipheriegerät **100** führt dann einen Einstellungsvorgang (d.h. einen Setup- oder Initialisierungsvorgang) zur Verwendung des erhaltenen bzw. erfassten elektronischen Zertifikats in dem Multifunktionsperipheriegerät **100** durch.

[0026] Die Hardwareanordnung bzw. -ausgestaltung des Multifunktionsperipheriegeräts 100 gemäß dem ersten Ausführungsbeispiel wird als Nächstes beschrieben.

[0027] **Fig. 2** ist ein Blockschaltbild zur Erläuterung der Hardwareanordnung bzw. -ausgestaltung des Multifunktionsperipheriegeräts **100** gemäß dem ersten Ausführungsbeispiel.

[0028] Eine CPU **201** führt ein Softwareprogramm des Multifunktionsperipheriegeräts 100 aus, um die Gesamtvorrichtung zu steuern bzw. zu betreiben. Ein ROM **202** ist ein Festwertspeicher und speichert Bootprogramme, feste Parameter und dergleichen für den Betrieb des Multifunktionsperipheriegeräts **100**. Ein RAM **203** ist ein Direktzugriffsspeicher und wird verwendet, um Programme und temporäre Daten zu speichern, wenn die CPU **201** das Mul-

tifunktionsperipheriegerät **100** steuert bzw. betreibt. Ein HDD **204** ist ein Festplattenlaufwerk und speichert Systemsoftware, Anwendungen und verschiedene andere Arten von Daten. Die CPU 201 steuert den Betrieb des Multifunktionsperipheriegeräts **100**, indem sie ein in dem ROM **202** gespeichertes Bootprogramm ausführt, ein in dem HDD **204** gespeichertes Programm in dem RAM **203** installiert bzw. anwendet, und das installierte bzw. angewandte Programm ausführt. Eine Netzwerkschnittstellensteuereinheit **205** steuert den Datenaustausch zwischen dem Netzwerk **110** und dem Multifunktionsperipheriegerät **100**. Eine Eingabeschnittstellensteuereinheit (z.B. eine Scannerschnittstellensteuereinheit **206**), steuert eine Bilddatenerfassung (z.B. ein Scannen oder Lesen eines Dokuments), das durch eine Eingabevorrichtung wie etwa einen Scanner **211** durchgeführt wird. Eine Ausgabeschnittstellensteuereinheit (z.B. eine Druckerschnittstelleneinheit **207**) steuert eine Datenausgabe (z.B. einen Druckprozess), die durch eine Ausgabevorrichtung wie etwa den Drucker **210** durchgeführt wird. Eine Anzeigesteuereinheit (z.B. eine Panelsteuereinheit **208**) steuert eine Anzeigevorrichtung und eine Eingabevorrichtung (z.B. ein Bedienpanel **212** des Berührungsfeldtyps), um ein Anzeigen von verschiedenen Arten von Informationen und ein Empfangen/Verarbeiten von durch einen Benutzer eingegebenen Anweisungen zu steuern. Die CPU **201**, der ROM **202**, der RAM **203**, das HDD **204**, die Netzwerkschnittstellensteuereinheit **205**, die Scannerschnittstellensteuereinheit **206**, die Druckerschnittstellensteuereinheit **207** und die Panelsteuereinheit **208** sind miteinander kommunikationsfähig, zum Beispiel sind sie durch einen Bus **209** miteinander verbunden. Steuersignale von der CPU **201** und Datensignale zwischen verschiedenen Komponenten der Vorrichtung werden über den Bus **209** ausgetauscht bzw. kommuniziert.

[0029] **Fig. 3** ist ein Blockschaltbild zur Erläuterung von Softwaremodulen, die in (z.B. funktionalen Komponenten von) Programmen umfasst sind, die auf dem Multifunktionsperipheriegerät **100** gemäß dem ersten Ausführungsbeispiel auszuführen sind oder laufen zu lassen sind. Es ist zu beachten, dass in **Fig. 3** gezeigte Softwaremodule zum Beispiel dadurch implementiert werden, dass die CPU **201** ein Programm in dem RAM **203** installiert bzw. anwendet und das installierte bzw. angewandte Programm ausführt.

[0030] Ein Netzwerktreiber **301** steuert die Netzwerkschnittstellensteuereinheit **205**, die mit dem Netzwerk **110** verbunden ist, und tauscht Daten über das Netzwerk **110** mit Außen aus (d.h. kommuniziert diese). Ein Netzwerksteuermodul **302** führt einen Datenaustausch durch Steuerung einer Kommunikation in der Transportschicht und den unteren Schichten in einem Netzwerkkommunikationsprotokoll wie etwa TCP/IP durch. Ein Kommunikationssteuermodul **303** ist ein Modul zum Steuern (und Implementieren) einer Vielzahl von Kommunikationsprotokollen, die durch das Multifunktionsperipheriegerät **100** unterstützt werden. In den Prozessen zur Erfassung und Aktualisierung des elektronischen Zertifikats gemäß dem ersten Ausführungsbeispiel macht (z.B. erzeugt und überträgt) das Kommunikationssteuermodul **303** eine HTTP-Protokoll-Kommunikationsanforderung, erzeugt es Antwortdaten, führt es eine Analyse durch, steuert es den Austausch von Daten, und führt es Prozesse für eine Kommunikation mit der Zertifizierungs-/Registrierungsstelle **102** und/oder dem PC **103** aus. Das Kommunikationssteuermodul **303** ist auch im Stande, eine verschlüsselte Kommunikation unter Verwendung von TLS, IPSEC und IEEE802.1X durchzuführen (z.B. indem es geeignete Prozesse bzw. Programme ausführt), falls eine solche durch das Multifunktionsperipheriegerät **100** unterstützt wird.

[0031] Ein Webseitensteuermodul **304** ist ein Modul, das HTML-Datenerzeugung und Kommunikationssteuerung durchführt, um eine Webseite anzuzeigen, die im Stande ist, die Elektronisches-Zertifikat-Ausstellungsanforderungs- und -erfassungsprozesse anzuweisen/auszuführen (z.B. indem es ein geeignetes Programm ausführt). Das Webseitensteuermodul **304** führt eine Verarbeitung für eine Webseitenanzeigeanforderung, eine Elektronisches-Zertifikat-Ausstellungsanforderung und eine Anweisung zum Ausführen/Aktivieren der Erfassung des ausgestellten elektronischen Zertifikats durch Übertragung/Empfang von diesem mit dem Kommunikationssteuermodul **303** über den Netzwerktreiber 301 aus/durch. Das Webseitensteuermodul **304** überträgt, als eine Antwort auf eine Anforderung, die von (unter Verwendung einer Eingabe, die gemacht wurde auf) dem Webbrowser gemacht wurde, die HTML-Daten einer vorbestimmten Webseite, die in dem RAM **203** und dem HDD **204** gespeichert sind, oder die HTML-Daten, die gemäß dem Inhalt einer Anzeigeanforderung (z.B. einer Anforderung zum Anzeigen von Detailinformationen eines elektronischen Zertifikats) erzeugt werden.

[0032] Ein Schlüsselpaar-Zertifikat-Erfassungsmodul **305** ist ein Modul zum Ausführen des Elektronisches-Zertifikat-Erfassungsprozesses basierend auf einer Anweisung von dem Webseitensteuermodul **304**. Das Schlüsselpaar-Zertifikat-Erfassungsmodul **305** ist ein Modul, das eine Kommunikationssteuerung mittels SCEP, eine Erzeugung verschlüsselter Daten und eine für eine Kommunikation unter Verwendung von SCEP notwendige Analyseverarbeitung wie etwa PKCS#7 und PKCS#10, sowie eine Verarbeitung zur Speicherung- und Anwendungseinstellung (z.B. Setup oder Initialisierung) des erfassten elektronischen Zertifikats durchführt. Ein Verschlüsselungsmodul **306** ist ein Modul, das verschiedene Arten von Verschlüsselungsprozessen wie etwa Da-

tenverschlüsselungs- und -entschlüsselungsprozesse, Erzeugung und Verifikation einer elektronischen Signatur und Hashwerterzeugung ausführt. In der Verarbeitung zur Erfassung und Aktualisierung des elektronischen Zertifikats gemäß dem ersten Ausführungsbeispiel führt das Verschlüsselungsmodul **306** Verschlüsselungsprozesse aus, die für die Erzeugung und Analyse von SCEP-Anforderungs-/Antwortdaten notwendig sind. Ein Schlüsselpaar-Zertifikat-Verwaltungsmodul **307** ist ein Modul, das öffentliche Schlüsselpaare bzw. Paare öffentlicher Schlüssel und elektronische Zertifikate verwaltet, die in dem Multifunktionsperipheriegerät **100** gehalten/gespeichert werden. Zum Beispiel speichert das Schlüsselpaar-Zertifikat-Verwaltungsmodul **307** das öffentliche Schlüsselpaar und die Daten von jedem elektronischen Zertifikat in dem RAM **203** und/oder dem HDD **204** zusammen mit verschiedenen Arten von Einstellwerten. Obgleich Prozesse für Detailinformationsanzeige, Erzeugung und Löschung des öffentlichen Schlüsselpaars und des elektronischen Zertifikats in **Fig. 3** nicht gezeigt sind, ist es möglich, die Prozesse basierend auf Benutzeranweisungen (die z.B. über das Bedienpanel **212** angenommen werden) auszuführen. Ein UI-Steuermodul **308** führt eine Steuerung des Bedienpanels **212** und der Panelsteuereinheit **208** aus/durch. Es ist zu beachten, dass gemäß diesem Ausführungsbeispiel selbst in dem Fall eines verschlüsselten Kommunikationsprozesses wie etwa TSL, IPSEC, IEEE802.1X, der durch das Kommunikationssteuermodul **303** ausgeführt wird, die Verschlüsselungsverarbeitung selbst in dem Verschlüsselungsmodul **306** durchgeführt wird, und die Daten des öffentlichen Schlüsselpaars und des elektronischen Zertifikats, die zu verwenden sind, von dem Schlüsselpaar-Zertifikat-Verwaltungsmodul **307** erfasst bzw. erhalten werden. Es ist jedoch selbstverständlich, dass andere Anordnungen bzw. Ausgestaltungen für die Verschlüsselungsprozesse und die Daten des öffentlichen Schlüsselpaars und des elektronischen Zertifikats ebenfalls möglich sind, solange funktional äquivalente oder kompatible Merkmale durch diese Anordnungen bzw. Ausgestaltungen bereitgestellt werden.

[0033] Ein Ausgabe-/Eingabeverarbeitungsmodul (z.B. ein Druck-/ Scanverarbeitungsmodul **309**) ist ein Modul zum Steuern der Ausführung von Ausgabe-/Eingabefunktionen wie etwa einer Datenausgabefunktion (z.B. Drucken durch den Drucker **210**) und einer Dateneingabefunktion (z.B. Dokumentlesen/- scannen durch den Scanner **211**). Ein Gerätesteuermodul **310** ist ein Modul zum (z.B. zentralen) Steuern des Multifunktionsperipheriegeräts **100** durch Erzeugung von Steuerbefehlen und Steuerdaten für den Betrieb des Multifunktionsperipheriegeräts **100**. Es ist zu beachten, dass das Verschlüsselungsmodul **306** gemäß dem ersten Ausführungsbeispiel Zugriff auf die Energieversorgung des Multifunktionsperipheriegeräts **100** hat, sodass es gegebenenfalls eine Neustartverarbeitung des Multifunktionsperipheriegeräts **100** basierend auf einer Anweisung von dem Webseitensteuermodul **304** ausführen kann.

[0034] **Fig. 4A** und **Fig. 4B** sind Sequenzdiagramme zur Erläuterung von Sequenzprozessschritten, die in einer Gesamtverarbeitung involviert sind, die in einer Netzwerkanordnung bzw. -ausgestaltung oder einem System gemäß dem ersten Ausführungsbeispiel durchgeführt wird. Der Ablauf beginnt mit einem anfänglichen Setup bzw. einer anfänglichen Initialisierung von Einstellungen in Bezug auf eine Ausstellungsanforderung für ein elektronisches Zertifikat, einem Anzeigen von Informationen über das elektronische Zertifikat, der Ausstellungsanforderung und einem Empfang des elektronischen Zertifikats, und geht dann weiter zu einer Aktivierung bzw. Ermöglichung einer Verwendung des elektronischen Zertifikats und einem Neustart des Multifunktionsperipheriegeräts.

[0035] Dieser Ablauf wird in Erwiderung auf eine Schlüsselpaar- und Elektronisches-Zertifikat-Liste-Anzeigeanweisung gestartet, die durch einen Benutzer eingegeben wird. Obgleich bei diesem Ausführungsbeispiel ein Beispiel der Prozesse beschrieben wird, die für ein Multifunktionsperipheriegerät **100** durchgeführt werden, können die gleichen Prozesse durch eine Vielzahl von Multifunktionsperipheriegeräten **100** und **101** in Erwiderung auf eine Startanweisung durchgeführt werden. Zum Beispiel kann eine Anforderung von dem PC **103** an jedes der Multifunktionsperipheriegeräte **100** und **101** übertragen werden, und können die Prozesse, die in den nachfolgenden Ablaufdiagrammen gemäß Fig. 5A bis **Fig. 9** gezeigt sind, in jedem Multifunktionsperipheriegerät ausgeführt werden. In einem solchen Fall können die Schritte, in denen ein Zertifikat in jedem der Multifunktionsperipheriegeräte **100** und **101** erfasst, angezeigt und bestätigt wird, ausgelassen werden. Auch kann ein Zertifikat mit abgelaufener Gültigkeitsdauer durch jedes Multifunktionsperipheriegerät automatisch detektiert werden, können die bibliographischen Informationen (eine Zertifikat-ID und die Gültigkeitsdauer) des abgelaufenen Zertifikats an den PC **103** übertragen werden, und kann der PC **103** die Vielzahl von Multifunktionsperipheriegeräten veranlassen, den Aktualisierungsprozess des Zertifikats automatisch auszuführen, das eine Gültigkeitsdauer hat, die gerade dabei ist abzulaufen oder bereits abgelaufen ist. Dieser vorgenannte Vorgang ist eine sogenannte stille Installation.

[0036] Als Erstes empfängt, in Schritt S401, auf Akzeptieren einer Verbindung von (d.h. Herstellen eines Kommunikationskanals mit) dem PC **103**, das Multifunktionsperipheriegerät **100**, von dem PC **103**, eine Anforderung zum Anzeigen der durch das Multifunktionsperipheriegerät **100** gehaltenen Schlüssel-

paar-/Elektronisches-Zertifikat-Liste. Bei dem ersten Ausführungsbeispiel sei angenommen, dass der Administrator des Multifunktionsperipheriegeräts **100** einen auf dem PC **103** installierten Webbrowser verwenden wird, um sich mit einer RUI im Webseitenformat zu verbinden, die verwendet wird, um eine Ausstellungsanforderung zu machen und ein durch das Multifunktionsperipheriegerät **100** veröffentlichtes elektronisches Zertifikat zu erfassen, und anweisungsbezogene Bedienungen (z.B. eine Eingabe einer Anweisung für einen Vorgang, der auf dem Multifunktionsperipheriegerät **100** oder **101** durchzuführen ist) durchführen wird. Dieses RUI ist ein Akronym für „Remote User Interface“ und stellt eine Technik dar, die es einem Benutzer ermöglicht, den Webbrowser von dem PC **103** zu verwenden, um von der Ferne eine Anforderung für Bedienbildschirmdaten des Multifunktionsperipheriegerät **100** oder **101** vorzunehmen, um den Bedienbildschirm auf dem PC 103 anzuzeigen. Als Beispiel ist es möglich, den Bildschirm unter Verwendung von HTML und Servlet zu implementieren.

[0037] Als Nächstes erfasst, in Schritt S402, das Multifunktionsperipheriegerät **100** Daten zum Anzeigen der Schlüsselpaar-/Elektronisches-Zertifikat-Liste, die in dem Multifunktionsperipheriegerät **100** gehalten wird, und führt es eine Webseitenbildschirm-Erzeugungsverarbeitung zum Anzeigen der erfassten Daten aus.

[0038] **Fig. 5A** ist ein Ablaufdiagramm zur Beschreibung von Prozessen, die in einer Schlüsselpaar-/Elektronisches-Zertifikat-Liste-Erfassung und Anzeigedatenerzeugung/-bildung in Schritt S402 von **Fig. 4A** involviert sind. Es ist zu beachten, dass diese Verarbeitung zum Beispiel dadurch implementiert wird, dass die CPU 201 ein in dem RAM **203** installiertes bzw. angewandtes Programm ausführt.

[0039] **Fig. 17A** bis **Fig. 17C** zeigen konzeptionelle Darstellungen der durch das Schlüsselpaar-Zertifikat-Verwaltungsmodul **307** verwalteten Schlüsselpaar-/ Elektronisches-Zertifikat-Detailinformationen-Datenbank. Gemäß diesem Ausführungsbeispiel wird/ist diese Datenbank in dem HDD **204** des Multifunktionsperipheriegeräts 100 gespeichert. Es ist jedoch selbstverständlich, dass diese Datenbank woanders gespeichert werden/sein kann, solange sie durch das Multifunktionsperipheriegerät **100** zugänglich ist, wenn dies notwendig ist.

[0040] Es wird nun das Ablaufdiagramm von **Fig. 5A** beschrieben. Diese Verarbeitung wird gestartet (eingeleitet bzw. initiiert), wenn eine Schlüsselpaar-/Elektronisches-Zertifikat-Liste-Erfassungsanforderung empfangen wird. Zunächst empfängt, in Schritt S501, die CPU **201** die Schlüsselpaar-/Elektronisches-Zertifikat-Liste-Erfassungsanforderung. Als Nächstes schreitet der Prozess zu Schritt S502 voran, und erfasst die CPU **201** zum Beispiel die in **Fig. 17A** gezeigten Detailinformationen des Schlüsselpaars bzw. elektronischen Zertifikats, das durch das Schlüsselpaar-Zertifikat-Verwaltungsmodul **307** verwaltet wird. Als Nächstes schreitet der Prozess zu Schritt S503 voran, und verwendet die CPU **201** die Detailinformationen des in Schritt S502 erfassten Schlüsselpaars bzw. elektronischen Zertifikats, um HTML-Daten für einen Webseitenbildschirm zu erzeugen, der als RUI bereitzustellen ist.

[0041] **Fig. 10A** bis **Fig. 15** zeigen Ansichten, die Beispiele der Webseitenbildschirme (d.h. RUIs) zeigen, die auf dem PC **103** gemäß dem ersten Ausführungsbeispiel anzuzeigen sind. In Schritt S503 von **Fig. 5** gemäß dem ersten Ausführungsbeispiel sei angenommen, dass die HTML-Daten für den in **Fig. 10A** gezeigten Webseitenbildschirm erzeugt werden, und dass die erzeugten HTML-Daten unter Verwendung des Webbrowsers von dem PC **103** angezeigt werden. Als Folge hiervon kann die durch das Multifunktionsperipheriegerät **100** gehaltene Schlüsselpaar-/Elektronisches-Zertifikat-Liste von dem PC **103** aus einfach bestätigt bzw. verifiziert werden.

[0042] Die Informationen des elektronischen Zertifikats, die in der Liste gemäß **Fig. 10A** angezeigt werden, umfassen einen Namen **1011**, eine Anwendung **1012**, einen Aussteller **1013**, einen Ablauf **1014** und ein Detail **1015** des Zertifikats. Der Name **1011** ist eine Zeichenkette, die durch einen Bediener wie etwa den Administrator des Multifunktionsperipheriegeräts **100** beliebig hinzugefügt wird, wenn das Schlüsselpaar bzw. elektronische Zertifikat ausgestellt wird. Die Anwendung 1012 ist ein Einstellwert, der bezeichnet, dass das Schlüsselpaar bzw. elektronische Zertifikat für eine Anwendung verwendet werden wird, die ein bestimmtes Kommunikationsprotokoll von TLS, IPSEC oder IEEE802.1X implementiert bzw. verwendet. Der Aussteller **1013** ist ein eindeutiger Name (DN: „Distinguished Name“) (d.h. eine Identifikation) von der CA, die das elektronische Zertifikat ausgestellt hat. Der Ablauf **1014** ist eine Information, die das Datum bezeichnet, an dem die Gültigkeitsdauer des elektronischen Zertifikats ablaufen wird. Das Detail **1015** ist ein Bildzeichen zum Anzeigen der detaillierten Informationen des elektronischen Zertifikats. Der Prozess schreitet danach zu Schritt S504 voran, und die CPU **201** überträgt, als eine Antwort auf Schritt S501, die in Schritt S503 erzeugten HTML-Daten an den PC **103** und beendet die Verarbeitung. Somit wird/ist Schritt S403 von **Fig. 4A** auf diese Art und Weise ausgeführt.

[0043] Es ist zu beachten, dass, obgleich dies in den Sequenzdiagrammen von **Fig. 4A** und **Fig. 4B** nicht gezeigt ist, eine Anforderung zum Anzeigen der Detailinformationen des elektronischen Zertifikats von dem PC **103** an das Multifunktionsperipheriege-

rät **100** übertragen wird, wenn der Administrator des Multifunktionsperipheriegeräts **100** auf das Bildzeichen des Details **1015** gemäß **Fig. 10A** klickt, wenn dies auf dem PC **103** angezeigt wird. Das Multifunktionsperipheriegerät 100, das diese Anzeigeanforderung empfangen hat, wird die Detailinformationen des elektronischen Zertifikats erfassen, die HTML-Daten für die Detailinformationen des Zertifikats basierend auf den erfassten Informationen erzeugen, und die erzeugten Daten als Antwort auf die Anzeigeanforderung an den PC **103** übertragen.

[0044] Als Folge hiervon werden die Detailinformationen des elektronischen Zertifikats auf dem Webbrowser von dem PC **103** zum Beispiel in der Art und Weise angezeigt, die in **Fig. 16** gezeigt ist. **Fig. 16** zeigt eine beispielhafte Ansicht der Detailinformationen des elektronischen Zertifikats, die auf dem PC **103** angezeigt werden.

[0045] **Fig. 5B** ist ein Ablaufdiagramm zur Beschreibung der Verarbeitung, die durchgeführt wird, wenn eine Anforderung zum Anzeigen dieser Detailinformationen von dem PC **103** durch das Multifunktionsperipheriegerät **100** gemäß dem ersten Ausführungsbeispiel empfangen wird. Es ist zu beachten, dass diese Verarbeitung zum Beispiel dadurch implementiert wird, dass die CPU **201** ein in dem RAM **203** installiertes bzw. angewandtes Programm ausführt.

[0046] Als Erstes empfängt, in Schritt S511, die CPU **201** eine Anforderung zum Erfassen der Detailinformationen des elektronischen Zertifikats von dem PC **103**. Als Nächstes schreitet der Prozess zu Schritt S512 voran, und erfasst die CPU **201** die in **Fig. 17A** gezeigten Detailinformationen des Schlüsselpaars bzw. elektronischen Zertifikats, das durch das Schlüsselpaar-Zertifikat-Verwaltungsmodul **307** verwaltet wird. Als Nächstes schreitet der Prozess zu Schritt S513 voran, und erzeugt die CPU **201** die HTML-Daten für einen Webseitenbildschirm durch Verwendung der in Schritt S512 erfassten Detailinformationen des Schlüsselpaars bzw. elektronischen Zertifikats, und überträgt sie die erzeugten HTML-Daten in Schritt S514 an den PC **103**.

[0047] **Fig. 16** zeigt eine Bildschirmansicht, die ein Beispiel der Anzeigebildschirmansicht der Detailinformationen des elektronischen Zertifikats gemäß dem ersten Ausführungsbeispiel zeigt. Diese Bildschirmansicht wird als RUI in einem Webseitenformat auf dem PC **103** angezeigt.

[0048] Wieder zu der Beschreibung von **Fig. 4A** zurückkehrend überträgt, in Schritt S403, das Multifunktionsperipheriegerät **100**, als eine Antwort auf eine Anforderung von dem PC **103**, die HTML-Daten für den in **Fig. 10A** gezeigten Webseitenbildschirm, die in Schritt S402 erzeugt werden.

[0049] Es ist zu beachten, dass die Prozesse, die in Schritt S402 bis Schritt S403 von Fig. 4A, Schritt S501 bis Schritt S504 von Fig. 5A und Schritt S511 bis Schritt S514 von **Fig. 5B** gezeigt sind, die vorstehend beschrieben sind, Steuerprozessschritte in Bezug auf die Elektronisches-Zertifikat-Informationen-Anzeigeverarbeitung darstellen, die durch das Multifunktionsperipheriegerät **100** durchgeführt werden, wenn eine Anforderung zum Anzeigen der Schlüsselpaar-/ Elektronisches-Zertifikat-Liste empfangen wird.

[0050] In Schritt S404 empfängt das Multifunktionsperipheriegerät **100** eine Anforderung zum Anzeigen eines Verbindungseinrichtungsbildschirms eines SCEP-Servers (eines Beispiels von einer CA/RA **102**) von dem PC **103**. Es sei angenommen, dass, um einen Verbindungseinrichtungsvorgang (z.B. eine Einstellung von Verbindungseinstellungen/-parametern zum Herstellen eines Kommunikationskanals bzw. einer Kommunikationsverbindung) mit der Zertifizierungs-/Registrierungsstelle **102** durchzuführen, der Administrator des Multifunktionsperipheriegeräts **100** gemäß dem ersten Ausführungsbeispiel auf in **Fig. 10A** gezeigte Verbindungseinstellungen **1002** klickt, um eine Verbindungseinrichtungsbildschirm-Anzeigeanforderung an das Multifunktionsperipheriegerät **100** zu übertragen.

[0051] Als Nächstes überträgt, in Schritt S405, das Multifunktionsperipheriegerät **100**, als eine Antwort auf die in Schritt S404 empfangene Anforderung, HTML-Daten für einen in **Fig. 10B** gezeigten vorbestimmten SCEP-Server-Verbindungseinrichtungsbildschirm an den PC **103**.

[0052] Der in **Fig. 10B** gezeigte Verbindungseinrichtungsbildschirm umfasst Eingabefelder für einen Servernamen bzw. eine Serveradresse **1016** und eine Portnummer 1017 zum Eingeben des SCEP-Server-Hostnamens (z.B. dessen IP-Adresse) und der Verbindungszielportnummer, sowie eine Einstellschaltfläche **1018** zum Anweisen/Angeben des Abschlusses des Einrichtungs-/Einstellungsprozesses, d.h. des Abschlusses einer Einstellung der Eingabeeinstellwerte, sodass diese für die Verbindung vorgenommen bzw. bewirkt werden können.

[0053] Als Nächste empfängt, in Schritt S406, das Multifunktionsperipheriegerät **100** eine Einstellungsanweisungsanforderung des Verbindungseinrichtungsvorgangs von dem PC **103**. Es sei angenommen, dass der Administrator des Multifunktionsperipheriegeräts **100** gemäß dem ersten Ausführungsbeispiel diese Einstellungsanweisungsanforderung von dem PC 103an das Multifunktionsperipheriegerät **100** überträgt, indem er nach Eingabe der notwendigen Informationen in Bezug auf den Servernamen **1016** und die Portnummer **1017** gemäß **Fig. 10B** auf die Einstellschaltfläche **1018** klickt.

[0054] Als Nächstes führt, in Schritt S407, das Multifunktionsperipheriegerät **100** den Verbindungseinrichtungsvorgang durch (d.h. stellt es die Verbindungseinstellungen gemäß den eingegebenen Informationen ein), und führt es die Erzeugung von Webseitenbildschirmdaten zum Anzeigen des Einstellungsprozesses und des Einstellungsergebnisses des Verbindungseinrichtungsvorgangs aus. In Schritt S408 überträgt das Multifunktionsperipheriegerät **100**, als eine Antwort auf die Anforderung von dem PC **103**, die HTML-Daten für den Webseitenbildschirm, der auf den in Schritt S407 erzeugten Webseitenbildschirmdaten basiert und in **Fig. 11A** gezeigt ist.

[0055] **Fig. 6** ist ein Ablaufdiagramm zur Beschreibung des Verbindungseinrichtungsprozesses zum Herstellen einer Verbindung bzw. Kommunikation mit der Zertifizierungs-/Registrierungsstelle **102**, der in Schritt S407 von **Fig. 4A** durch das Multifunktionsperipheriegerät **100** gemäß dem ersten Ausführungsbeispiel durchgeführt wird. Es ist zu beachten, dass die Verarbeitung zum Beispiel dadurch implementiert wird, dass die CPU **201** ein in dem RAM **203** installiertes bzw. angewandtes Programm ausführt.

[0056] Als Erstes empfängt, in Schritt S601, die CPU **201** eine Verbindungseinstellungsanforderung von dem PC **103**. Als Nächstes schreitet der Prozess zu Schritt S602 voran, und erfasst die CPU **201** die Einstellwerte, z.B. den Hostnamen und die Portnummer, die in der Verbindungseinstellungsanforderung umfasst sind, und speichert sie die erfassten Einstellwerte in dem RAM **203** oder dem HDD **204**. Als Nächstes schreitet der Prozess zu Schritt S603 voran, und erzeugt die CPU **201** zum Beispiel die HTML-Daten für den in **Fig. 11A** gezeigten Webseitenbildschirm. Der Prozess schreitet zu Schritt S604 voran, und die CPU **201** überträgt die in Schritt S603 erzeugten HTML-Daten an den PC **103** als eine Antwort auf die Anforderung in Schritt S601 und beendet die Verarbeitung. Der Prozess schreitet auf diese Weise zu Schritt S408 voran.

[0057] Als Folge hiervon wird, wie es in **Fig. 11A** gezeigt ist, eine Zeichenkette **1101** auf dem PC **103** angezeigt, die bezeichnet, dass die Einstellungen implementiert wurden (d.h. die Einstellwerte zur Herstellung einer Verbindung mit der CA/RA 102 eingestellt/angewandt/bewirkt sind).

[0058] Die Prozesse, die in Schritt S406 bis Schritt S408 und Schritt S601 bis Schritt S604 gezeigt sind, die vorstehend beschrieben sind, sind die Steuervorgänge in Bezug auf den Verbindungseinrichtungsprozess des Multifunktionsperipheriegeräts **100**.

[0059] Als Nächstes empfängt, in Schritt S409 von Fig. 4A, das Multifunktionsperipheriegerät eine Anforderung zum Anzeigen des CA-Zertifikat-Erfassungsbildschirms, die von dem Browser von dem PC **103** übertragen wird. Bei dem ersten Ausführungsbeispiel sei angenommen, dass die Anforderung zum Anzeigen des CA-Zertifikat-Erfassungsbildschirms an das Multifunktionsperipheriegerät **100** übertragen wird, wenn der Administrator auf CA-Zertifikat-Erfassung **1003** klickt, was in **Fig. 10A** gezeigt ist, da der Administrator des Multifunktionsperipheriegeräts 100 das durch die Zertifizierungs-/Registrierungsstelle **102** ausgestellte CA-Zertifikat erfassen wird.

[0060] Als Folge hiervon überträgt, in Schritt S410, das Multifunktionsperipheriegerät 100, als eine Antwort auf die in Schritt S409 empfangene Anforderung, HTML-Daten des in **Fig. 11B** gezeigten vorbestimmten CA-Zertifikat-Erfassungsbildschirms.

[0061] Der in **Fig. 11B** gezeigte Verbindungseinstellungsbildschirm umfasst eine Ausführungsschaltfläche **1102** zum Anweisen der tatsächlichen Erfassung des CA-Zertifikats.

[0062] Als Nächstes empfängt, in Schritt S411, das Multifunktionsperipheriegerät **100** die CA-Zertifikat-Erfassungsanforderung, die von dem Browser von dem PC **103** übertragen wird, wenn die in **Fig. 11B** gezeigte Ausführungsschaltfläche **1102** angeklickt wird. Bei dem ersten Ausführungsbeispiel sei angenommen, dass die CA-Zertifikat-Erfassungsanforderung an das Multifunktionsperipheriegerät **100** übertragen wird, wenn der Administrator des Multifunktionsperipheriegeräts **100** die in **Fig. 11B** gezeigte Ausführungsschaltfläche **1102** anklickt.

[0063] Als Nächstes führt, in Schritt S412, das Multifunktionsperipheriegerät **100** eine Verarbeitung zum Erzeugen von CA-Zertifikat-Erfassungsanforderungsdaten aus/durch. Der Prozess schreitet zu Schritt S413 voran, und das Multifunktionsperipheriegerät **100** überträgt die in Schritt S412 erzeugten CA-Zertifikat-Erfassungsanforderungsdaten an die Zertifizierungs-/Registrierungsstelle **102**, die als der SCEP-Server dient, basierend auf den Informationen, die in dem in Schritt S407 durchgeführten Verbindungseinrichtungsvorgang eingestellt werden. Der Prozess schreitet zu Schritt S414 voran, und das Multifunktionsperipheriegerät **100** empfängt eine CA-Zertifikat-Erfassungsantwort, die von der Zertifizierungs-/Registrierungsstelle **102** übertragen wird. Als Folge hiervon analysiert, in Schritt S415, das Multifunktionsperipheriegerät **100** die empfangene CA-Zertifikat-Erfassungsantwort, erfasst sie das in der Antwort umfasste CA-Zertifikat, und führt sie eine Verarbeitung zum Registrieren des erfassten CA-Zertifikats als ein CA-Zertifikat durch, das für das Multifunktionsperipheriegerät 100 zuverlässig bzw. vertrauenswürdig ist. Das Multifunktionsperipheriegerät **100** erzeugt auch HTML-Daten für einen Webseitenbildschirm zum Angeben eines Ergebnisses/Ausgangs des Vornehmens der CA-Zertifikat-Erfas-

sungsanforderung. Der Prozess schreitet zu Schritt S416 voran, und das Multifunktionsperipheriegerät **100** überträgt eine Antwort, die ein CA-Zertifikat-Erfassungsanforderungsergebnis umfasst, an den PC **103**. Die Antwort umfasst die HTML-Daten für den Webseitenbildschirm, der in Schritt S415 erzeugt wird und in **Fig. 12A** oder **Fig. 12B** gezeigt ist, als Indikatoren bzw. Hinweise des Ergebnisses (d.h. des Ausgangs des Vornehmens der Anforderung). **Fig. 12A** zeigt ein Beispiel eines Bildschirms, der angezeigt wird, wenn die Erfassung des CA-Zertifikats erfolgreich war und das erfasste Zertifikat als das zuverlässige bzw. vertrauenswürdige CA-Zertifikat registriert ist. Andererseits zeigt **Fig. 12B** ein Beispiel eines Bildschirms, der angezeigt wird, wenn die Erfassung des CA-Zertifikats fehlgeschlagen ist.

[0064] Fig. 7 ist ein Ablaufdiagramm zur ausführlicheren Beschreibung der Prozesse zur Erfassung und Registrierung des CA-Zertifikats, die in Schritt S412 bis S416 von **Fig. 4A** gezeigt sind und durch das Multifunktionsperipheriegerät **100** gemäß dem ersten Ausführungsbeispiel durchgeführt werden. Es ist zu beachten, dass diese Prozesse zum Beispiel dadurch implementiert werden, dass die CPU **201** ein in dem RAM **203** installiertes bzw. angewandtes Programm ausführt.

[0065] Als Erstes empfängt, in Schritt S701, die CPU **201** eine CA-Zertifikat-Erfassungsanforderung von dem PC **103**. Als Nächstes schreitet der Prozess zu Schritt S702 voran, und erzeugt die CPU **201** eine CA-Zertifikat-Erfassungsanforderungsnachricht basierend auf den für eine Verbindung bzw. Kommunikation mit der Zertifizierungs-/Registrierungsstelle **102** eingestellten Informationen zur Verbindungseinstellung(-einrichtung), die in Schritt S407 erfasst wurden. Ein Beispiel der Erfassungsanforderungsnachricht, die gemäß dem ersten Ausführungsbeispiel erzeugt wird, ist nachstehend gezeigt. Da SCEP als das Kommunikationsprotoll bei dem ersten Ausführungsbeispiel verwendet wird, wird die folgende Nachricht als eine Anforderungsnachricht unter Verwendung dieses Protokolls verwendet.
xxxxxxx/yyyyy?operation=GetCAXyz&message=
CAIdentifier

[0066] Als Nächstes schreitet der Prozess zu Schritt S703 voran, und die CPU **201** steuert die Netzwerkschnittstellensteuereinheit **205** zum Verbinden mit der Zertifizierungs-/Registrierungsstelle **102**, die als der SCEP-Server dient, mittels des TCP/IP-Protokolls basierend auf den Verbindungseinstellungsinformationen für die Zertifizierungs-/Registrierungsstelle **102**, die in Schritt S407 von **Fig. 4A** erfasst wurden. Als Nächstes schreitet der Prozess zu Schritt S704 voran, und die CPU **201** bestimmt, ob die Verbindung in Schritt S703 erfolgreich war oder nicht. Wenn die Verbindung erfolgreich war, schreitet der Prozess zu Schritt S705 voran. Anderenfalls schreitet der Prozess zu Schritt S714 voran, um einen Fehlerverarbeitungsschritt durchzuführen.

[0067] In Schritt S705 überträgt die CPU **201** die in Schritt S702 erzeugte CA-Zertifikat-Erfassungsanforderungsnachricht an die Zertifizierungs-/Registrierungsstelle **102** zum Beispiel unter Verwendung des GET- oder POST-Verfahrens des HTTP-Protokolls. Als Nächstes schreitet der Prozess zu Schritt S706 voran, und bestimmt die CPU **201**, ob die Übertragung in Schritt S705 erfolgreich war oder nicht. Wenn die Übertragung erfolgreich war, schreitet der Prozess zu Schritt S707 voran. Anderenfalls schreitet der Prozess zu Schritt S714 für die Fehlerverarbeitung voran. In Schritt S707 empfängt die CPU **201** (über die Netzwerkschnittstellensteuereinheit **205**) Antwortdaten von der Zertifizierungs-/ Registrierungsstelle **102**, die als eine Antwort auf die CA-Zertifikat-Erfassungsanforderungsnachricht gesendet werden. Der Prozess schreitet zu Schritt S708 voran, und die CPU **201** bestimmt, ob der Empfang der Antwortdaten in Schritt S707 erfolgreich war oder nicht. Wenn der Empfang erfolgreich war, schreitet der Prozess zu Schritt S709 voran. Anderenfalls schreitet der Prozess zu Schritt S714 voran. In Schritt S709 analysiert die CPU **201** die in Schritt S707 empfangenen Antwortdaten, und erfasst sie die Daten des CA-Zertifikats, die in den Antwortdaten umfasst sind. Die Analyse dieser Antwortdaten und der Erfassungsprozess für das CA-Zertifikat werden durch das Verschlüsselungsmodul **306** durchgeführt.

[0068] Es ist zu beachten, dass die Antwortdaten gemäß dem ersten Ausführungsbeispiel binäre Daten in einem X.509-Format sind (RFC5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile). Jedoch können Daten zum Beispiel ebenso in einem PKCS#7-Format (RFC 5652: Cryptographic Message Syntax) als eine Antwort übertragen werden, und ist es selbstverständlich, dass das Datenformat nicht auf ein bestimmtes beschränkt ist, solange das CA-Zertifikat aus diesem erfasst bzw. erhalten werden kann.

[0069] Der Prozess schreitet zu Schritt S710 voran, und die CPU **201** bestimmt, ob die Erfassung des CA-Zertifikats in Schritt S709 erfolgreich war oder nicht. Wenn die Erfassung erfolgreich war, schreitet der Prozess zu Schritt S711 voran. Anderenfalls schreitet der Prozess zu Schritt S714 voran. In Schritt S711 registriert die CPU **201** das in Schritt S709 erfasste CA-Zertifikat als ein CA-Zertifikat, das für das Multifunktionsperipheriegerät **100** zuverlässig bzw. vertrauenswürdig ist. Die CPU **201** hält (speichert vorübergehend) das erfasste CA-Zertifikat in dem RAM 203 und veranlasst das Schlüsselpaar-Zertifikat-Verwaltungsmodul **307** zum Speichern des CA-Zertifikats in einem vorbestimmten Verzeichnis von dem HDD 204 zur Speicherung des CA-Zertifikats, das

für das Multifunktionsperipheriegerät **100** zuverlässig bzw. vertrauenswürdig ist. Der Prozess schreitet zu Schritt S712 voran, und die CPU **201** bestimmt, ob der CA-Zertifikat-Registrierungsprozess in Schritt S711 erfolgreich war oder nicht. Wenn der Prozess erfolgreich war, schreitet der Prozess zu Schritt S713 voran. Anderenfalls schreitet der Prozess zu Schritt S714 voran. In Schritt S713 erzeugt die CPU **201** einen Daumenabdruck (einen Hashwert, der unter Verwendung eines SHA1-Algorithmus erhalten wird) von dem CA-Zertifikat, der in einer Art und Weise anzuzeigen ist, wie es durch eine Zeichenkette **1201** von **Fig. 12A** angedeutet ist, wenn die Erfassung und Registrierung des CA-Zertifikats erfolgreich waren. Die Erzeugung dieses Daumenabdrucks wird durch das Verschlüsselungsmodul **306** ausgeführt/durchgeführt. Der Prozess schreitet dann zu Schritt S715 voran, und die CPU **201** erzeugt, basierend auf den Verarbeitungsergebnissen von Schritt S703 bis Schritt S714, HTML-Daten für CA-Zertifikat-Erfassungsergebnisanzeigedaten, die, je nachdem, in Fig. 12A oder **Fig. 12B** gezeigt sind. Der Prozess schreitet zu Schritt S716 voran, und die CPU **201** nimmt eine Steuerung zum Übertragen der in Schritt S715 erzeugten HTML-Daten, an den PC **103**, als eine Antwort auf die in S701 empfangene Anforderung vor und beendet die Erfassungs- und Registrierungsverarbeitung. Danach schreitet der Prozess zu Schritt S417 von **Fig. 4A** voran. Bei dem ersten Ausführungsbeispiel wird die Zeichenkette **1201** von **Fig. 12A** gemäß dem CA-Zertifikat-Erfassungs- und Registrierungsergebnis angezeigt. Alternativ wird, wenn die Fehlerverarbeitung in Schritt S714 ausgeführt wird, zum Beispiel eine Zeichenkette **1202** von **Fig. 12B** angezeigt. Als Nächstes wird die Beschreibung zu **Fig. 4A** zurückkehren.

[0070] In Schritt S417 empfängt das Multifunktionsperipheriegerät **100** eine Anforderung, die von dem Browser von dem PC **103** übertragen wird, zum Anzeigen des Zertifikatsausstellungsanforderungsbildschirms. Bei dem ersten Ausführungsbeispiel sei angenommen, dass der Administrator des Multifunktionsperipheriegeräts 100 auf eine Zertifikatsausstellungsanforderung **1004**, die in **Fig. 10A** gezeigt ist, klicken wird, um eine Zertifikatsausstellungsanforderung an die Zertifizierungs-/ Registrierungsstelle **102** vorzunehmen, um ein neu ausgestelltes elektronisches Zertifikat zu erfassen bzw. erhalten.

[0071] Als Nächstes überträgt, in Schritt S418, das Multifunktionsperipheriegerät **100**, als eine Antwort auf die Anzeigeanforderung in Schritt S417, HTML-Daten für einen vorbestimmten Zertifikatsausstellungsbildschirm, von dem ein Beispiel in **Fig. 13A** gezeigt ist, an den PC **103**. Als Folge hiervon führt der PC **103** eine Anzeigesteuerung zum Anzeigen des in **Fig. 13A** gezeigten Bildschirms durch.

[0072] Der Zertifikatsausstellungsanforderungsbildschirm gemäß **Fig. 13A** umfasst einen Namen **1301** des Zertifikats, eine Schlüssellänge **1302** zum Einstellen einer Schlüssellänge für ein zu erzeugendes Schlüsselpaar, ein Ausstellungszielinformationen-Eingabefeld **1303**, eine Signaturverifikation **1304**, die bezeichnet, ob eine Signatur, die zu einer von der Zertifizierungs-/Registrierungsstelle **102** übertragenen Zertifikatsausstellungsanforderungsantwort hinzuzufügen ist, zu verifizieren/authentisieren ist, eine Schlüsselanwendung **1305** zum Einstellen der Anwendung von (d.h. dem Kommunikationsprotokoll, das zu verwenden ist mit) dem ausgestellten Zertifikat, ein Passwort **1306**, das in die Zertifikatsausstellungsanforderung einzufügen ist, und eine Ausführungsschaltfläche **1307** zum Ausführen/Anweisen der Zertifikatsausstellungsanforderungsübertragung. Bei diesem Ausführungsbeispiel wird die Schlüsselanwendung **1305** als eine Gruppe von Ankreuzfeldern bzw. -kästchen eingestellt, und zeigt sie, dass es möglich ist, eine Vielzahl von Anwendungen (d.h. mehr als ein Kommunikationsprotokoll) für ein Zertifikat einzustellen.

[0073] Als Nächstes empfängt, in Schritt S419, wenn die Zertifikatsausstellungsanforderung angewiesen wird, zum Beispiel durch Klicken auf die Ausführungsschaltfläche **1307** des in **Fig. 13A** gezeigten Bildschirms, das Multifunktionsperipheriegerät **100** die Zertifikatsausstellungsanforderung, die Elemente von Eingabe-/ Einstellungsinformationen/-daten umfasst, die mit den durch jeweilige Bezugszeichen **1301** bis **1306** bezeichneten Objekten in Zusammenhang stehen, die von dem Browser von dem PC **103** eingestellt werden. Bei dem ersten Ausführungsbeispiel sei angenommen, dass der Administrator des Multifunktionsperipheriegeräts **100** die Informationen eingibt und einstellt, die mit den Objekten in Zusammenhang stehen, die durch die jeweiligen Bezugszeichen **1301** bis **1306** bezeichnet sind, und auf die in **Fig. 13A** gezeigte Ausführungsschaltfläche **1307** klickt, um die Zertifikatsausstellungsanforderungsanweisung von dem PC **103** an das Multifunktionsperipheriegerät **100** zu übertragen.

[0074] Als Nächstes führt, in Schritt S420, das Multifunktionsperipheriegerät **100** den Prozess zur Erzeugung der Zertifikatsausstellungsanforderung (-daten) aus/durch. In Schritt S421 überträgt das Multifunktionsperipheriegerät **100**, basierend auf den in Schritt S407 eingestellten Informationen, die in Schritt S420 erzeugten Zertifikatsausstellungsanforderungsdaten an die Zertifizierungs-/ Registrierungsstelle **102**, die als der SCEP-Server dient. Die Zertifizierungs-/ Registrierungsstelle **102** stellt dann das Zertifikat basierend auf Ausstellungsanforderungsdaten aus und überträgt eine Zertifikatsausstellungsanforderungsantwort. In Schritt S422 empfängt das Multifunktionsperipheriegerät **100** die von der Zertifizierungs-/Registrierungsstelle **102** übertragene Zer-

tifikatsausstellungsanforderungsantwort. Als Nächstes führt, in Schritt S423, das Multifunktionsperipheriegerät **100** Analyse- und Registrierungsprozesse (Ausführen/Durchführen einer Signaturverifikation/-authentisierung gemäß der Einstellung, Erfassen des in der Antwort umfassten Zertifikats, und Einstellen/Registrieren des erfassten Zertifikats für die bezeichnete/spezifizierte Anwendung, d.h. das spezifizierte Kommunikationsprotokoll) von der in Schritt S422 empfangenen Zertifikatsausstellungsanforderungsantwort durch. Danach führt das Multifunktionsperipheriegerät **100** einen Webseitenbildschirm-Erzeugungsprozess zum Anzeigen des Ergebnisses der Zertifikatsausstellungsanforderung aus.

[0075] Wenn die Zertifikatsausstellung und die darauffolgende Erfassung des ausgestellten Zertifikats erfolgreich waren, wird hier eine Speicherung und eine Anwendungseinstellung (z.B. eine Kommunikationsprotokolleinstellung) der Elektronisches-Zertifikat-Daten durch die Verarbeitung in Schritt S423 durchgeführt. Hier bezieht sich die Anwendungseinstellung auf eine Einstellung von Einstellungen/Parametern für die Kommunikationsfunktion, die das elektronische Zertifikat verwendet, und führt die verschlüsselten Kommunikationsprotokolle wie etwa TLS, IPSEC und IEEE802.1X, die bei dem ersten Ausführungsbeispiel einstellbar/konfigurierbar (d.h. zur Verwendung abhängig von einer Einstellung verfügbar) sind. Auch sei angenommen, dass ein Multifunktionsperipheriegerät **100** gemäß dem ersten Ausführungsbeispiel eine Vielzahl von elektronischen Zertifikaten halten/speichern kann und ein oder mehr Anwendungen (z.B. ein oder mehr Kommunikationsprotokolle) für jedes elektronische Zertifikat einstellen kann. Zum Beispiel sind verschiedene Anwendungen (z.B. Kommunikationsprotokolle) einstellbar, wenn ein elektronisches Zertifikat, das durch das Multifunktionsperipheriegerät **100** zum Bereitstellen eines Serverdiensts (mittels Durchführung einer TLS-Kommunikation zum Dienen als ein Webserver) verwendet wird, und ein elektronisches Zertifikat, das durch das Multifunktionsperipheriegerät 100 zum Durchführen einer Clientkommunikation (z.B. unter Verwendung von IEEE802.1X) verwendet wird, voneinander verschieden sind. Es ist jedoch selbstverständlich, dass auch ein einziges elektronisches Zertifikat für alle oder mehr als eine der Kommunikationsanwendungen angewandt/verwendet werden kann, soweit dies angemessen ist.

[0076] In Schritt S424 überträgt das Multifunktionsperipheriegerät **100**, an den PC **103**, HTML-Daten des in Fig. 13B oder **Fig. 14A** erzeugten Webseitenbildschirms, der in Schritt S423 erzeugt wurde. Es ist zu beachten, dass eine Einstellungsergebnis-Zeichenkette, wie sie durch eine Zeichenkette **1308** in Fig. 13B und eine Zeichenkette **1401** in **Fig. 14A** gezeigt ist, gemäß dem Zertifikatsausstellungsanforderungsergebnis angezeigt werden wird. **Fig. 13B** zeigt eine Ansicht, die ein Beispiel eines Bildschirms veranschaulicht, wenn Zertifikatsausstellung und -erfassung erfolgreich waren. Der in **Fig. 13B** gezeigte Bildschirm wird auf dem PC **103** in einem Fall angezeigt, in dem eine Zertifikatsausstellungsanforderung von dem PC **103** an das Multifunktionsperipheriegerät **100** übertragen wird und das Zertifikat gemäß der Ausstellungsanforderung ausgestellt wird. Das ausgestellte Zertifikat wird als ein Zertifikat eingestellt, das durch das Multifunktionsperipheriegerät **100** zum Durchführen einer gesicherten bzw. geschützten Kommunikation verwendet wird, wenn das Multifunktionsperipheriegerät **100** neu gestartet wird. Auf dem in **Fig. 13B** gezeigten Bildschirm ist eine Nachricht umfasst, die einen Benutzer anhält bzw. mahnt, das Multifunktionsperipheriegerät **100** neu zu starten. **Fig. 14A** zeigt eine Ansicht, die ein Beispiel einer Bildschirmansicht veranschaulicht, wenn Zertifikatsausstellung und -erfassung fehlgeschlagen sind. Der in **Fig. 14A** gezeigte Bildschirm wird auf dem PC **103** in einem Fall angezeigt, in dem eine Zertifikatsausstellungsanforderung von dem PC **103** an das Multifunktionsperipheriegerät **100** übertragen wird, aber das Zertifikat nicht ausgestellt wird. Auf dem in **Fig. 14A** gezeigten Bildschirm ist eine Nachricht umfasst, die einen Benutzer über ein Fehlschlagen einer Ausstellung des Zertifikats benachrichtigt.

[0077] Wenn Zertifikatsausstellung und -erfassung auf diese Art und Weise erfolgreich waren, wird durch den Prozess in Schritt S423 eine Speicherung und eine Anwendungs-(Kommunikationsprotokoll-)einstellung der Elektronisches-Zertifikat-Daten durchgeführt. Da das Kommunikationssteuermodul **303** gemäß dem ersten Ausführungsbeispiel die Elektronisches-Zertifikat-Daten, die in der verschlüsselten Kommunikation wie etwa TLS, IPSEC und IEEE802.1X verwendet werden, zu der Zeit einer Aktivierung des Multifunktionsperipheriegeräts **100** (d.h. wenn das Kommunikationssteuermodul **303** während des Starts bzw. der Inbetriebnahme des Multifunktionsperipheriegeräts 100einen verschlüsselten Kommunikationskanal initialisiert und herstellt, der das Kommunikationsprotokoll verwendet) erfasst, ist ein Neustart des Multifunktionsperipheriegerät **100** notwendig, wenn die Änderungen in der Anwendung (dem Kommunikationsprotokoll und dem zugehörigen elektronischen Zertifikat) zu bewirken/implementieren sind).

[0078] **Fig. 8A** und **Fig. 8B** sind Ablaufdiagramme zur ausführlicheren Beschreibung der Verarbeitung der Zertifikatsausstellungsanforderung/-erfassung, die in Schritt S419 bis Schritt S424 von **Fig. 4B** durch das Multifunktionsperipheriegerät **100** gemäß dem ersten Ausführungsbeispiel durchgeführt wird. Es ist zu beachten, dass diese Verarbeitung zum Beispiel dadurch implementiert wird, dass die CPU 201 ein in dem RAM installiertes bzw. angewandtes Programm ausführt.

[0079] Als Erstes empfängt, in Schritt S801, die CPU **201** eine Zertifikatsausstellungsanforderung von dem PC **103** (z.B. über die Netzwerkschnittstellensteuereinheit 205). Als Nächstes schreitet der Prozess zu Schritt S802 voran, und erfasst die CPU **201** Einstellwerte der Anforderung, z.B. die Informationen über den Namen 1301 des Zertifikats, die Schlüssellänge **1302**, das Ausstellungszielinformationen-Eingabefeld **1303**, die Signaturverifikation **1304** und die Schlüsselanwendung 1305, die in der in Schritt S801 empfangenen Zertifikatsausstellungsanforderung umfasst sind. Als Nächstes schreitet der Prozess zu Schritt S803 voran, und erfasst die CPU **201** das CA-Zertifikat, das in Schritt S412 bis Schritt S415 von **Fig. 4A** erfasst wird. Der Prozess schreitet zu Schritt S804 voran, und die CPU **201** führt eine Verarbeitung durch, um ein Schlüsselpaar basierend auf den Informationen von dem Namen **1301** und der Schlüssellänge **1302** zu erzeugen, die in Schritt S802 erfasst werden, und Daten einer Zertifikatssignierungsanforderung (CSR: „Certificate Signing Request“) eines PKCS#10-Formats (RFC2986: PKCS#10: Certification Request Syntax Specification) basierend auf den Informationen von dem Ausstellungszielinformationen-Eingabefeld **1303** und dem Passwort **1306** unter Verwendung des Verschlüsselungsmoduls **306** zu erzeugen. Als Nächstes schreitet der Prozess zu Schritt S805 voran, und bestimmt die CPU 201, ob die Erzeugung von dem Schlüsselpaar/CSR in Schritt S804 erfolgreich war oder nicht. Wenn bestimmt wird, dass die Erzeugung erfolgreich war, schreitet der Prozess zu Schritt S806 voran. Anderenfalls schreitet der Prozess zu Schritt S823 voran, um eine Fehlerverarbeitung durchzuführen. In Schritt S806 erzeugt die CPU **201** Zertifikatsausstellungsanforderungsdaten (z.B. die CSR-Daten). Die in Schritt S806 erzeugten CSR-Daten werden zu den PKCS#7-Format-Daten, die in dem SCEP definiert sind, basierend auf den in Schritt S407 von **Fig. 4A** erfassten Verbindungseinstellungen, die zur Kommunikation mit der Zertifizierungs-/Registrierungsstelle **102** eingestellt sind. Als Nächstes schreitet der Prozess zu Schritt S807 voran, und bestimmt die CPU **201**, ob eine Datenerzeugung in Schritt S806 dahingehend erfolgreich war oder nicht, die Zertifikatsausstellungsanforderungsdaten zu erzeugen. Wenn die Datenerzeugung erfolgreich war, schreitet der Prozess zu Schritt S808 voran. Anderenfalls schreitet der Prozess zu Schritt S823 voran.

[0080] In Schritt S808 führt die CPU **201** eine TCP/IP-Protokoll-Verbindung zu der Zertifizierungs-/Registrierungsstelle **102**, die als ein SCEP-Server dient, basierend auf der Verbindungseinstellung für die Zertifizierungs-/Registrierungsstelle **102** aus, die in Schritt S407 von **Fig. 4A** erfasst wurde. Als Nächstes schreitet der Prozess zu Schritt S809 voran, und bestimmt die CPU **201**, ob die Verbindung in Schritt S808 erfolgreich war oder nicht. Wenn die Verbindung erfolgreich war, schreitet der Prozess zu Schritt S810 voran. Anderenfalls schreitet der Prozess zu Schritt S823 voran. In Schritt S810 überträgt die CPU **201** die in Schritt S806 erzeugten CSR-Daten durch das GET- oder POST-Verfahren des HTTP-Protokolls an die Zertifizierungs-/Registrierungsstelle **102**. In Schritt S811 bestimmt die CPU **201**, ob die Übertragung in Schritt S810 erfolgreich war oder nicht. Wenn die Übertragung erfolgreich war, schreitet der Prozess zu Schritt S812 voran. Anderenfalls schreitet der Prozess zu Schritt S823 voran. In Schritt S812 empfängt die CPU 201 (z.B. über die Netzwerkschnittstellensteuereinheit **205**) eine Zertifikatsausstellungsantwort (die z.B. CSR-Antwortdaten umfasst) von der Zertifizierungs-/ Registrierungsstelle **102**. Die Antwortdaten sind durch das SCEP definiert, und PKCS#7-Format-Daten werden als Antwort übertragen. Es ist selbstverständlich, dass andere Datenformate ebenfalls verwendet werden können.

[0081] Als Nächstes schreitet der Prozess zu Schritt S813 voran, und bestimmt die CPU 201, ob ein Empfang der Antwortdaten in Schritt S812 erfolgreich war oder nicht. Wenn der Empfang erfolgreich war, schreitet der Prozess zu Schritt S814 voran. Anderenfalls schreitet der Prozess zu Schritt S823 voran. In Schritt S814 bestimmt die CPU **201**, ob eine Signaturverifikation erforderlich ist oder nicht, z.B. durch Bestimmung, ob eine Signaturverifikationseinstellung vorhanden ist, basierend auf den Informationen über die Signaturverifikation **1304**, die in Schritt S802 erfasst werden. Wenn die Signaturverifikation durchzuführen ist, schreitet der Prozess zu Schritt S815 voran. Anderenfalls schreitet der Prozess zu Schritt S817 voran. In Schritt S815 nimmt die CPU **201** eine Steuerung zum Verifizieren/Authentisieren der Signaturdaten, die zu den in Schritt S812 empfangenen Antwortdaten hinzugefügt sind, unter Verwendung des öffentlichen Schlüssels vor, der in dem in Schritt S803 erfassten CA-Zertifikat umfasst ist. Der Prozess schreitet zu Schritt S816 voran, und die CPU **201** bestimmt, ob das Ergebnis der Signaturverifikation in Schritt S815 erfolgreich war (d.h. die Signatur als authentisch/gültig verifiziert/authentisiert wurde) oder nicht. Wenn die Signaturverifikation erfolgreich war, schreitet der Prozess zu Schritt S817 voran. Anderenfalls schreitet der Prozess zu Schritt S823 voran.

[0082] In Schritt S817 nimmt die CPU **201** eine Steuerung zum Analysieren der in Schritt S812 empfangenen Antwortdaten und Erfassen von in den Antwortdaten umfassten Zertifikatsdaten vor. Die Prozesse zur Antwortdatenanalyse und Zertifikatserfassung werden zum Beispiel durch das Verschlüsselungsmodul **306** durchgeführt. Als Nächstes bestimmt, in Schritt S818, die CPU **201**, ob eine Zertifikatserfassung in Schritt S817 erfolgreich war oder nicht. Wenn die Zertifikatserfassung erfolgreich war, schreitet der Prozess zu Schritt S819 voran. Anderenfalls schreitet der Prozess zu Schritt S823 vor-

an. In Schritt S819 registriert die CPU **201** das in Schritt S818 erfasste Zertifikat als das elektronische Zertifikat (d.h. digitale Zertifikat), das dem in Schritt S804 erzeugten Schlüsselpaar entspricht. Zu der gleichen Zeit veranlasst/steuert die CPU **201** das Schlüsselpaar-Zertifikat-Verwaltungsmodul **307** zum Speichern des in Schritt S804 erzeugten öffentlichen Schlüsselpaars und des erfassten elektronischen Zertifikats in einem vorbestimmten Verzeichnis von dem HDD **204** zur Speicherung des Schlüsselpaars bzw. elektronischen Zertifikats. Das Schlüsselpaar-Zertifikat-Verwaltungsmodul **307** fügt auch die Informationen über das in Schritt S804 erzeugte öffentliche Schlüsselpaar und das erfasste elektronische Zertifikat zu der Liste von Schlüsselpaar-Zertifikat-Detailinformationen hinzu, wie es in **Fig. 17B** gezeigt ist. Gemäß **Fig. 17B** wurde ein neues Schlüsselpaar bzw. Zertifikat Xyz4 hinzugefügt.

[0083] Als Nächstes schreitet der Prozess zu Schritt S820 voran, und bestimmt die CPU 201, ob der Zertifikatsregistrierungsprozess in Schritt S819 erfolgreich war oder nicht. Wenn die Registrierung erfolgreich war, schreitet der Prozess zu Schritt S821 voran. Anderenfalls schreitet der Prozess zu Schritt S823 voran. In Schritt S821 stellt die CPU **201** Einstellungen für eine Anwendung, die das Zertifikat verwenden werden wird, basierend auf den in Schritt S802 erfassten Informationen über die Schlüsselanwendung **1305** ein. Zum Beispiel aktualisiert das Schlüsselpaar-Zertifikat-Verwaltungsmodul **307** die Anwendungsinformationen (z.B. Informationen über das Kommunikationsprotokoll) in der Liste von Schlüsselpaar-/Elektronisches-Zertifikat-Detailinformationen, wie es in **Fig. 17C** gezeigt ist. Gemäß **Fig. 17C** wurde das in TLS zu verwendendes Schlüsselpaar bzw. Zertifikat von Xyz1 (gemäß **Fig. 17B**) auf Xyz4 geändert Als Nächstes schreitet der Prozess zu Schritt S822 voran. Die CPU **201** bestimmt, ob die Anwendungseinstellung (z.B. Aktualisierung des elektronischen Zertifikats) in Schritt S821 erfolgreich war oder nicht. Wenn die Anwendungseinstellung (z.B. die Aktualisierung) erfolgreich war, schreitet der Prozess zu Schritt S824 voran. Anderenfalls schreitet der Prozess zu Schritt S823 voran.

[0084] In Schritt S824 erzeugt die CPU **201** HTML-Daten für das Zertifikatsausstellungsanforderungsergebnis, wie es in **Fig. 13B** gezeigt ist, das einem Ergebnis/Ausgang der Verarbeitung von Schritt S801 bis Schritt S823 entspricht. In Schritt S825 nimmt die CPU **201** eine Steuerung zum Übertragen der in Schritt S824 erzeugten HTML-Daten an den PC **103** als eine Antwort auf die Zertifikatsausstellungsanforderung von Schritt S801 vor, und beendet sie die Verarbeitung zur Zertifikatsausstellungsanforderung/-erfassung. Danach schreitet der Prozess zu Schritt S425 von **Fig. 4B** voran.

[0085] Die Prozesse von Schritt S419 bis Schritt S424 und Schritt S801 bis Schritt S825, die vorstehend beschrieben sind, bilden Teile von Steuervorgängen in Bezug auf die Verarbeitung der Elektronisches-Zertifikat-Ausstellungsanforderung und deren Antwort und der Einstellung der Kommunikations-(Protokoll-)anwendung des Multifunktionsperipheriegeräts **100**. Bei dem ersten Ausführungsbeispiel werden diese Prozesse, die von der Verarbeitung der Ausstellungsanforderung und -antwort bis zu der Kommunikationsprotokollanwendungseinstellung durchgeführt worden, kollektiv als „die automatische Elektronisches-Zertifikat-Aktualisierungsfunktion“ bezeichnet.

[0086] Durch Ausführung dieser automatischen Elektronisches-Zertifikat-Aktualisierungsfunktion kann das Multifunktionsperipheriegerät **100** die Verarbeitung der Elektronisches-Zertifikat-Ausstellungsanforderung und -antwort über das Netzwerk automatisch durchführen und auch die Anwendung (z.B. das Kommunikationsprotokoll) des empfangenen elektronischen Zertifikats einstellen. Dies kann die Arbeitsbelastung des Benutzers verringern. Die Beschreibung wird zu **Fig. 4B** zurückkehren.

[0087] In Schritt S425 empfängt das Multifunktionsperipheriegerät **100** eine Anforderung zum Neustarten des Multifunktionsperipheriegeräts **100**. Bei dem ersten Ausführungsbeispiel sei angenommen, dass der Administrator des Multifunktionsperipheriegeräts **100** das Multifunktionsperipheriegerät **100** neu startet, indem er auf eine in **Fig. 13B** gezeigte Neustartschaltfläche **1309** klickt.

[0088] Als Nächstes schreitet der Prozess zu Schritt S426 voran, und überträgt das Multifunktionsperipheriegerät **100**, als eine Antwort auf die Neustartanforderung in Schritt S425, HTML-Daten des vorbestimmten Neustartausführungsbildschirms, der zum Beispiel in **Fig. 14B** gezeigt ist. Als Nächstes schreitet der Prozess zu Schritt S427 voran, und führt das Multifunktionsperipheriegerät **100** den Neustartprozess für das Multifunktionsperipheriegerät **100** aus/durch.

[0089] Das Multifunktionsperipheriegerät **100** gemäß dem ersten Ausführungsbeispiel wurde unter der Annahme beschrieben, dass ein Neustart notwendig ist, um jedwede Änderungen, die an den Anwendungseinstellungen vorgenommen werden, vorzunehmen bzw. zu bewirken, z.B. wenn ein Kommunikationsprotokoll (eine Anwendung) für das empfangene elektronische Zertifikat auf IEEE802.1X eingestellt wird. Dies ist deshalb so, da zum Beispiel ein elektronisches Zertifikat für IEEE802.1X zu der Zeit einer Aktivierung bzw. eines Starts oder einer Inbetriebnahme des Multifunktionsperipheriegeräts **100** in dem RAM **203** installiert/angewandt bzw. initialisiert werden kann und fortwährend in Verwendung sein

kann, was bedeutet, dass es nicht durch das empfangene elektronische Zertifikat ersetzt werden kann, das in dem HDD **204** gespeichert wurde. Wenn es jedoch möglich ist, das elektronische Zertifikat, das für die Anwendung unter Verwendung des bestimmten Kommunikationsprotokolls zu verwenden ist, ohne den Neustart des Multifunktionsperipheriegeräts **100**, zu wechseln bzw. zu ändern, kann es so eingestellt sein, dass der Neustart nicht durchgeführt wird. Zum Beispiel, wenn die Anwendung für TLS eingestellt ist, kann es so eingestellt sein, dass der Neustart als unnötig erachtet wird. Zum Beispiel ist es möglich, einen Indikator bzw. Hinweis hinsichtlich der Notwendigkeit eines Neustarts für jede von der Vielzahl von Anwendungen vorab einzustellen, und kann das Multifunktionsperipheriegerät **100** gemäß Informationen dieses Neustartnotwendigkeitsindikators- bzw. -hinweises automatisch bestimmen, ob neu zu starten ist. In einem weiteren Beispiel kann der PC **103** derartige Informationen eines Neustartnotwendigkeitsindikators bzw. -hinweises speichern und basierend darauf bestimmen, ob die Neustartanforderung an das Multifunktionsperipheriegerät **100** zu übertragen ist oder nicht.

[0090] **Fig. 9** ist ein Ablaufdiagramm zur Beschreibung der Prozesse in Bezug auf den Neustart des Multifunktionsperipheriegeräts **100** in Schritt S425 bis Schritt S427 von Fig. 4B, die durch das Multifunktionsperipheriegerät **100** gemäß dem ersten Ausführungsbeispiel durchgeführt werden. Es ist zu beachten, dass diese Verarbeitung zum Beispiel dadurch implementiert wird, dass die CPU **201** ein in dem RAM **203** installiertes bzw. angewandtes Programm ausführt.

[0091] Als Erstes empfängt, in Schritt S901, die CPU **201** eine Anforderung zum Neustarten des Multifunktionsperipheriegeräts **100** von dem PC **103** (z.B. über die Netzwerkschnittstellensteuereinheit **205**). Als Nächstes schreitet der Prozess zu Schritt S902 voran, und die CPU **201** überträgt (z.B. über die Netzwerkschnittstellensteuereinheit **205**), an den PC **103**, als eine Antwort auf die Neustartanforderung in Schritt S901, vorbestimmte HTML-Daten für die Neustartanforderung des Multifunktionsperipheriegeräts **100**, die in **Fig. 14B** gezeigt sind. Als Nächstes schreitet der Prozess zu Schritt S903 voran. Die CPU **201** wird das Gerätesteuermodul **310** anweisen/veranlassen/steuern, den Neustartprozess zu starten, und beendet die Neustartverarbeitung.

[0092] Mittels Durchführung der vorstehend beschriebenen Sequenz von Vorgängen ist es möglich, das von der Zertifizierungs-/Registrierungsstelle **102** erfasste elektronische Zertifikat in dem neu gestarteten Multifunktionsperipheriegerät **100** zu verwenden.

[0093] **Fig. 15** zeigt eine Darstellung, die ein Beispiel einer Bildschirmansicht zeigt, wenn die Schlüsselpaar-/Elektronisches-Zertifikat-Liste durch Ausführung der Verarbeitung von Schritt S401 bis Schritt S403 erneut angezeigt wird, nachdem die Zertifikatsausstellung und -erfassung erfolgreich waren. Informationen **1501** des Zertifikats Xyz4, das durch die Zertifizierungs-/Registrierungsstelle **102** neu ausgestellt ist, wurden zu dieser Liste hinzugefügt.

[0094] Die Gesamtprozesssequenz von den Prozessschritten für die anfängliche Einrichtung (Einstellung) in Bezug auf die Elektronisches-Zertifikat-Ausstellungsanforderung, die Anzeige der Informationen hinsichtlich des elektronischen Zertifikats, die Ausstellungsanforderung und den Empfang des ausgestellten elektronischen Zertifikats, bis zu dem Prozess zum Neustarten des Multifunktionsperipheriegeräts und Vornehmen/Implementieren/Aktivieren des ausgestellten elektronischen Zertifikats gemäß dem ersten Ausführungsbeispiel wurden vorstehend beschrieben.

[0095] Es ist zu beachten, dass, obgleich die Sequenz der in **Fig. 4A** und **Fig. 4B** gezeigten Verarbeitung mit den Prozessen, die von der anfänglichen Verbindungseinrichtung in Schritten S404-S408 bis zu der Ausstellungsanforderung und dem Vornehmen/Implementieren/Aktivieren des ausgestellten elektronischen Zertifikats in Schritten S419-S427 involviert sind, als eine einzige serielle Sequenz von Vorgängen beschrieben wurde, die Prozesse in Bezug auf den anfänglichen Verbindungseinrichtungsvorgang (Schritte S401-S418), wie etwa die Verbindungseinstellung in Schritten S404-S408, nur einmal für das Multifunktionsperipheriegerät **100** durchgeführt werden können und danach nicht wiederholt werden, sofern nicht ein spezielles Erfordernis für eine Verbindung mit einer anderen CA oder eine Aktualisierung in den Verbindungseinstellwerten auftritt. Zum Beispiel können die Einstellungsvorgänge des Anzeigens der Elektronisches-Zertifikat-Informationen in Schritt S401 bis Schritt S403, der anfängliche Verbindungseinrichtungsprozess in Schritt S404 bis Schritt S408 und der CA-Zertifikat-Erfassungsprozess von Schritt S409 bis Schritt S418 nur für die erste Zertifikatsausstellungsanforderung durchgeführt werden. Dann kann ein Betrieb so vorgenommen werden, dass die gleichen Einstellungen für die zweite und jede folgende Elektronisches-Zertifikat-Ausstellungsanforderung verwendet werden. Mit anderen Worten kann zu der Zeit der Durchführung der zweiten oder jeder folgenden Elektronisches-Zertifikat-Aktualisierung/Ausstellung ein Betrieb so vorgenommen werden, dass nur die Verarbeitungsschritte in Bezug auf die Verarbeitung der Elektronisches-Zertifikat-Ausstellungsanforderung und deren Antwort und die Prozesse in Bezug auf die Kommunikationsanwendungseinstellungen in Schritt S419 bis Schritt S424 und, falls erforderlich, die Neustart- und Implementierungs-/Aktivierungsverar-

beitung von Schritt S425 bis Schritt S427 ausgeführt werden.

[0096] Bei dem ersten Ausführungsbeispiel empfängt das Multifunktionsperipheriegerät 100 Verarbeitungsanweisungen von dem PC **103** über die RUIs im Webseitenformat, die durch das Multifunktionsperipheriegerät **100** selbst gehalten werden (d.h. darin gespeichert sind), und führt es Steuerungen basierend auf diesen Anweisungen durch. Die Schnittstelle, die verwendet wird zum Annehmen einer Anweisung von dem Administrator an das Multifunktionsperipheriegerät **100**, ist jedoch nicht besonders auf eine solche Anordnung bzw. Ausgestaltung beschränkt. Jede Anweisung kann anstelle von jeder RUI im Webseitenformat zum Beispiel von einer lokalen Benutzerschnittstelle (LUI: „Local User Interface“) angenommen werden, die auf dem Multifunktionsperipheriegerät **100** selbst oder einer anderen Vorrichtung bereitgestellt ist, die mit dem Multifunktionsperipheriegerät **100** verbunden ist (z.B. dem Drucker **210** oder dem Scanner **211**), wobei der durch das Multifunktionsperipheriegerät **100** gehaltene Drucker verwendet wird.

[0097] Zusätzlich kann stattdessen, dass der Administrator eine Anforderung manuell vornimmt, indem er die RUI im Webseitenformat direkt bedient, eine Anordnung bzw. Ausgestaltung vorliegen, dass eine Anforderung von einem PC oder einem anderen Verwaltungsserver automatisch an bzw. für das Multifunktionsperipheriegerät **100** eingegeben und angewiesen werden kann, indem zum Beispiel ein Template bzw. eine Vorlage für jeden Webseiteneingabebereich und eine Regel für jede Webseitenbedienungsanweisung im Voraus erzeugt werden. In diesem Fall kann zum Beispiel eine Web-Scraping-(Data-Mining-)Technik verwendet werden.

[0098] Obgleich das erste Ausführungsbeispiel eine Anordnung bzw. Ausgestaltung aufweist, in der der Vorgang zum Erfassen und Registrieren eines CA-Zertifikats durch den Administrator des Multifunktionsperipheriegeräts **100** durchgeführt wird, kann es auch eine Anordnung bzw. Ausgestaltung aufweisen, in der das CA-Zertifikat, wenn dies erforderlich ist, zu der Zeit der ersten oder jeder folgenden Zertifikatsausstellungsanforderung automatisch erfasst wird.

[0099] Auch war das erste Ausführungsbeispiel mit einer Signaturverifikationseinstellung (zum Bezeichnen, ob eine Signaturverifikation durchzuführen ist) versehen, die in der Zertifikatsausstellungsanforderungsantwort von der Zertifizierungs-/ Registrierungsstelle **102** umfasst ist. Anstelle der Bereitstellung dieser einstellbaren/regelbaren Einstellung kann sie jedoch voreingestellt sein, sodass die Signaturverifikation immer durchgeführt wird oder die Signaturverifikation nicht durchgeführt wird.

[0100] Obgleich das erste Ausführungsbeispiel eine Anordnung bzw. Ausgestaltung aufweist, in der ein Passwort als Daten in der Zertifikatsausstellungsanforderung umfasst ist (z.B. das Passwort in der CSR umfasst ist), kann es außerdem eine Anordnung bzw. Ausgestaltung aufweisen, in der das Passwort unnötig ist (z.B. nicht verwendet wird).

[0101] Wie es vorstehend beschrieben ist, kann gemäß dem ersten Ausführungsbeispiel eine Zertifikatshinzufügungs-/-aktualisierungsanforderung (z.B. die Zertifikatsausstellungsanforderung) an eine externe Vorrichtung wie etwa eine Zertifizierungs-/ Registrierungsstelle durch Verwendung eines automatischen Zertifikatsaktualisierungsprotokolls (d.h. der automatischen Elektronisches-Zertifikat-Aktualisierungsfunktion) basierend auf einer Anweisung von einer RUI abgegeben werden. Dann kann ein Zertifikat basierend auf der der Anforderung entsprechenden Antwort in dem Multifunktionsperipheriegerät empfangen und registriert werden, und können verschiedene Einstellungen oder Parameter zum Ausführen bzw. Laufenlassen einer Anwendung unter Verwendung des Zertifikats eingestellt werden.

[Zweites Ausführungsbeispiel]

[0102] Als Nächstes wird das zweite Ausführungsbeispiel der vorliegenden Erfindung beschrieben. Bei dem vorstehend dargelegten ersten Ausführungsbeispiel wurde eine RUI im Webseitenformat an den Benutzer des Multifunktionsperipheriegeräts 100 durch Verwendung der durch das Multifunktionsperipheriegerät **100** gehaltenen Webserverfunktion bereitgestellt. Der Benutzer hat verschiedene Einstellungen oder Parameter zum Ausführen bzw. Laufenlassen einer Anwendung, die das elektronische Zertifikat verwenden soll, hinzugefügt, aktualisiert und eingestellt, indem er Anweisungen über die RUI an das Multifunktionsperipheriegerät **100** gegeben hat. Da dieses elektronische Zertifikat eine Gültigkeitsdauer hat, ist ein elektronisches Zertifikat, für das die Gültigkeitsdauer abgelaufen ist, deaktiviert bzw. gesperrt. Dies kann eine Netzwerkkommunikation unterbrechen, da eine korrekte Kommunikationsauthentisierung mit einem deaktivierten bzw. gesperrten elektronischen Zertifikat nicht durchgeführt werden kann. Wenn die Gültigkeitsperiode des elektronischen Zertifikats, das durch eine Vorrichtung gehalten wird (in dieser gespeichert ist), nahe ihrer Ablaufzeit bzw. ihres Ablaufdatums ist oder abgelaufen ist, muss das elektronische Zertifikat daher aktualisiert werden. Wenn eine Vielzahl von Vorrichtungen vorhanden ist, die das elektronische Zertifikat verwenden, ist es für den Administrator der Vorrichtungen jedoch schwierig, die Gültigkeitsdauer des elektronischen Zertifikats von jeder Vorrichtung zu erhalten bzw. abzurufen bzw. zu erkennen bzw. zu erfassen und jedes elektronische Zertifikat individuell bzw. dementsprechend zu aktualisieren.

[0103] Daher wird das zweite Ausführungsbeispiel, in einer Informationsverarbeitungsvorrichtung, die im Stande ist, eine automatische Elektronisches-Zertifikat-Aktualisierungsfunktion durchzuführen, wie diejenige bei dem ersten Ausführungsbeispiel, einen Steuer-/Verwaltungsvorgang beschreiben, der die Elektronisches-Zertifikat-Aktualisierungsfunktion an einem vorbestimmten Datum und zu einer vorbestimmten Zeit (d.h. zu einer reservierten Zeit) automatisch aktiviert, anstelle jede Aktualisierung basierend auf einer Benutzeranweisung manuell zu steuern. Es ist zu beachten, dass bei dem zweiten Ausführungsbeispiel die Netzwerkanordnung bzw. -ausgestaltung, die Hardwareanordnung bzw. -ausgestaltung, die Softwareanordnung bzw. -ausgestaltung, die Anzeigeverarbeitung der Schlüsselpaar-/Elektronisches-Zertifikat-Liste, der Verbindungseinrichtungsprozess des Multifunktionsperipheriegeräts **100** als die Informationsverarbeitungsvorrichtung gleich denjenigen des ersten Ausführungsbeispiels sind und eine Beschreibung von diesen ausgelassen wird.

[0104] Fig. 18 zeigt eine Darstellung, die ein Beispiel eines Elektronisches-Zertifikat-Aktualisierungsreservierung-Einstellungsbildschirms zeigt, der für das Multifunktionsperipheriegerät **100** gemäß dem zweiten Ausführungsbeispiel bereitgestellt wird. Dieser Bildschirm wird zum Beispiel durch eine RUI im Webseitenformat auf die gleiche Art und Weise wie die anderen Bildschirme angezeigt, die hierin beschrieben sind. Ein Aktualisierungsdatum und eine Aktualisierungszeit (d.h. eine reservierte oder vorbestimmte Zeit) für das elektronische Zertifikat kann über diesen Elektronisches-Zertifikat-Aktual isierungsreservierung-Einstellungsbildschirm eingestellt werden. Bei dem zweiten Ausführungsbeispiel ist es möglich, als das Aktualisierungsdatum und die Aktualisierungszeit (und gegebenenfalls eine Aktualisierungsintervallbezeichnung), drei Einstellungen einzustellen: Aktualisierungsdatum und -zeit 1801; Zeitperiode **1802** vor dem Ablauf der Gültigkeitsdauer; und Zeitperiode zwischen Intervallen oder Datum zum Definieren eines Zyklus **1803**. Bei Aktualisierungsdatum und -zeit 1801 können das Jahr, der Monat, der Tag und die Zeit für die Aktualisierung eingestellt werden, und die automatische Elektronisches-Zertifikat-Aktualisierungsfunktion wird ausgeführt, wenn die aktuelle Zeit, die in dem Multifunktionsperipheriegerät **100** gehalten (z.B. durch dieses beobachtet/gemessen) wird, auf die eingestellte Zeit und das eingestellte Datum von diesem/dieser Aktualisierungsdatum und -zeit 1801 wechselt. Die Zeitperiode **1802** bezeichnet eine Anzahl von Tagen vor dem Ablauf der Gültigkeitsdauer des aktuell verwendeten elektronischen Zertifikats. Wenn die Tage von der/dem aktuellen Zeit und Datum, die in dem Multifunktionsperipheriegerät **100** gehalten (d.h. durch dieses beobachtet/gemessen) werden, bis zu der Gültigkeitsdauer, gleich oder weniger der Anzahl von Tagen werden, die durch die Zeitperiode **1802** bezeichnet sind, wird die automatische Elektronisches-Zertifikat-Aktualisierungsfunktion ausgeführt. Die Zeitperiode bzw. das Datum **1803** führt die automatische Elektronisches-Zertifikat-Aktualisierungsfunktion basierend auf einem Zyklus aus, wie er durch diese Zeitperiode bzw. dieses Datum definiert wird. Bei dem zweiten Ausführungsbeispiel kann dieser Zyklus basierend auf einer vorbestimmten Anzahl von Tagen (d.h. einer Zeitdauer), einem vorbestimmten Tag jedes Monats oder einem vorbestimmten Tag und einen vorbestimmten Monat jedes Jahres (d.h. Datum) eingestellt werden. Diese Einstellung (oder Reservierung) des/der Aktualisierungsdatums und -zeit oder des Aktualisierungszyklus der Aktualisierung von jedem elektronischen Zertifikat wird als „eine Elektronisches-Zertifikat-Aktualisierungsreservierungseinstellung“ bezeichnet. Wenn die Aktualisierungsreservierungseinstellung von jedem elektronischen Zertifikat aktualisiert wird, speichert die CPU **201** die aktualisierten Reservierungsinformationen in einem HDD 204.

[0105] Fig. 18 zeigt, in der Zeitperiode **1802**, ein Beispiel eines Bildschirms, wo eingestellt wurde, die automatische Elektronisches-Zertifikat-Aktualisierungsfunktion auszuführen, wenn das Datum zu 14 Tagen vor dem Ablauf der Gültigkeitsdauer wird. Obgleich die vorstehend beschriebenen Typen einer Elektronisches-Zertifikat-Aktualisierungsreservierungeinstellung verwendet werden, um eine Reservierung zum Durchführen des/der automatischen Elektronisches-Zertifikat-Aktualisierungsvorgangs/-funktion bei dem zweiten Ausführungsbeispiel vorzunehmen, ist es selbstverständlich, dass die vorliegende Erfindung nicht darauf beschränkt ist. Es kann auch eine andere Bezeichnungs-/Reservierungsmethode für Zeit und/oder Datum oder Zeitvorgabe verwendet werden, solange diese eine Bedingung oder einen Zeitpunkt bzw. eine Zeitdauer zum Durchführen/Ausführen dieses Vorgangs definieren kann.

[0106] Fig. 19 ist ein Ablaufdiagramm zur Beschreibung der Verarbeitung, die durchgeführt wird, wenn die automatische Elektronisches-Zertifikat-Aktualisierungsfunktion basierend auf der Elektronisches-Zertifikat-Aktualisierungsreservierungseinstellung auszuführen ist, die an dem Multifunktionsperipheriegerät **100** gemäß dem zweiten Ausführungsbeispiel eingestellt wird/ist. Obgleich hier ein Beispiel gezeigt ist, in dem die automatische Aktualisierungsfunktion für das Multifunktionsperipheriegerät **100** eingestellt wurde, ist es möglich, den in **Fig. 19** gezeigten Prozess auf einer Vielzahl von Multifunktionsperipheriegeräten auszuführen, indem die Vielzahl von Multifunktionsperipheriegeräten bezeichnet werden (ist es auch möglich, eine andere Zeit oder eine andere Bedingung zum Durchführen/Ausführen des automatischen Aktuali-

sierungsvorgangs für jedes Multifunktionsperipheriegerät einzustellen). In diesem Fall werden die Prozesse gemäß **Fig. 19** unter der Vielzahl von Multifunktionsperipheriegeräten parallel ausgeführt. Es ist zu beachten, dass die Verarbeitung zum Beispiel dadurch implementiert wird, dass die CPU **201** ein in einem RAM 203 installiertes bzw. angewandtes Programm ausführt.

[0107] Als Erstes erfasst, in Schritt S1901, die CPU **201** die Elektronisches-Zertifikat-Aktualisierungsreservierungseinstellung von dem HDD **204**. Als Nächstes schreitet der Prozess zu Schritt S1902 voran, und die CPU **201** erfasst die Informationen über das aktuell verwendete elektronische Zertifikat. Diese Informationen sind Informationen, wie etwa diejenigen, die in **Fig. 17A** bis **Fig. 17C** angedeutet sind. Als Nächstes schreitet der Prozess zu Schritt S1903 voran, und die CPU **201** erfasst die aktuelle Zeit und das aktuelle Datum, die durch das Multifunktionsperipheriegerät **100** beobachtet/gemessen werden. Es ist selbstverständlich, dass Zeitdifferenzen zwischen unterschiedlichen Zeitzonen hier ebenfalls berücksichtigt werden können. Als Nächstes schreitet der Prozess zu Schritt S1904 voran, und die CPU **201** vergleicht die Elektronisches-Zertifikat-Aktualisierungsreservierungseinstellung und die erfassten Elektronisches-Zertifikat-Informationen, um zu bestimmen, ob das aktuell verwendete elektronische Zertifikat aktualisiert werden muss oder nicht. Wenn bestimmt wird, dass das elektronische Zertifikat nicht aktualisiert werden muss, kehrt der Prozess hier zu Schritt S1901 zurück. Der Prozess kann für eine vorbestimmte Periode, oder bis eine andere vorbestimmte Bedingung erfüllt wurde, vor Rückkehr zu Schritt S1901 warten. Andererseits schreitet der Prozess, wenn bestimmt wird, dass das elektronische Zertifikat aktualisiert werden muss, zu Schritt S1905 und zu der in **Fig. 8A** und **Fig. 8B** beschriebenen Steuerung der „Zertifikatsausstellungsanforderungsverarbeitung“ voran. Nachdem die Verarbeitung gemäß **Fig. 8A** und **Fig. 8B** abgeschlossen ist, schreitet der Prozess zu Schritt S1906 voran.

[0108] Gemäß dem vorstehend beschriebenen Prozess ist es möglich, das elektronische Zertifikat basierend auf einem/einer bezeichneten bzw. voreingestellten Aktualisierungsdatum und -zeit oder einem Aktualisierungszyklus ohne manuelle Anweisung von dem Benutzer automatisch zu aktualisieren. Dies ermöglicht, dass das elektronische Zertifikat von jeder Vorrichtung aufrechterhalten wird, d.h. zu einer gewünschten Zeit-/vorgabe aktualisiert wird, während die Arbeitsbelastung des Benutzers verringert wird, und ohne zu erfordern, dass der Administrator die Gültigkeitsdauer des elektronischen Zertifikats von jeder Vorrichtung erfasst/erkennt/bestimmt.

[0109] In Schritt S1906 bestimmt die CPU **201**, auf Aktualisierung des elektronischen Zertifikats hin, ob das Multifunktionsperipheriegerät **100** neu gestartet werden muss. Wenn die CPU **201** bestimmt, dass ein Neustart notwendig ist, schreitet der Prozess hier zu Schritt S1907 voran, um den in **Fig. 9** gezeigten „Neustart-/ Einstellungsimplementierungs-/Aktivierungsprozess“ auszuführen. Andererseits, wenn die CPU **201** bestimmt, dass der Neustart nicht notwendig ist, beendet sie die Verarbeitung des automatischen Aktualisierungsvorgangs. Dies dient dazu, den Neustart des Multifunktionsperipheriegeräts **100** zu steuern, sodass dieses nur dann neu gestartet wird, wenn es notwendig ist. Zum Beispiel unterscheidet dies zwischen Fällen, in denen das Multifunktionsperipheriegerät **100** das zu verwendende elektronische Zertifikat umgeschaltet bzw. gewechselt hat und die Netzwerkkonfiguration für TLS geändert wird/ist, was einen Neustart nicht erfordert, und für IEEE 802.1X geändert wird/ist, was einen Neustart erfordert.

[0110] Wie es vorstehend beschrieben ist, ist es gemäß dem zweiten Ausführungsbeispiel durch Reservieren/Spezifizieren/Definieren der Aktualisierungszeitvorgabe des elektronischen Zertifikats für das Multifunktionsperipheriegerät möglich, eine Elektronisches-Zertifikat-Ausstellungsanforderung zum Aktualisieren und Registrieren eines elektronischen Zertifikats ohne Benutzeranweisung automatisch zu übertragen. Als Folge hiervon ist es möglich, eine Situation zu verhindern, in der das elektronische Zertifikat deaktiviert bzw. gesperrt wird/ist (z.B. weil es abgelaufen ist) und die Netzwerkkommunikation unterbrochen wird, selbst wenn der Benutzer von der Gültigkeitsdauer des elektronischen Zertifikats keine Kenntnis hat (z.B. aufgrund dessen, dass er keinen Zugriff auf ein solches Wissen bzw. eine solche Information hat).

Weitere Ausführungsbeispiele

[0111] Ausführungsbeispiele der vorliegenden Erfindung können auch verwirklicht werden durch einen Computer eines Systems oder einer Vorrichtung, der computerausführbare Anweisungen (z.B. ein oder mehr Programme), die auf einem Speichermedium (das vollständiger auch als ein „(nicht-vorübergehendes) computerlesbares Speichermedium“ bezeichnet werden kann) aufgezeichnet sind, ausliest und ausführt, um die Funktionen von ein oder mehr der vorstehend beschriebenen Ausführungsbeispiele durchzuführen, und/oder ein oder mehr Schaltungen (z.B. anwendungsspezifische integrierte Schaltung (ASIC)) zur Durchführung der Funktionen von ein oder mehr der vorstehend beschriebenen Ausführungsbeispiele umfasst, sowie durch ein Verfahren, das durch den Computer des Systems oder der Vorrichtung durchgeführt wird, indem dieser zum Beispiel die computerausführbaren Anweisungen von dem Speichermedium ausliest und ausführt, um die Funktionen von ein oder mehr der vorstehend beschriebenen Aus-

führungsbeispiele durchzuführen, und/oder die ein oder mehr Schaltungen steuert, um die Funktionen von ein oder mehr der vorstehend beschriebenen Ausführungsbeispiele durchzuführen. Der Computer kann ein oder mehr Prozessoren (z.B. Zentralverarbeitungseinheit (CPU), Mikroverarbeitungseinheit (MPU)) aufweisen und kann ein Netzwerk separater Computer oder separater Prozessoren umfassen, um die computerausführbaren Anweisungen auszulesen und auszuführen. Die computerausführbaren Anweisungen können an den Computer zum Beispiel von einem Netzwerk oder dem Speichermedium bereitgestellt werden. Das Speichermedium kann zum Beispiel ein oder mehr von einer Festplatte, einem Direktzugriffsspeicher (RAM), einem Festwertspeicher (ROM), einem Speicher verteilter Rechensysteme, einer optischen Platte (wie etwa einer Compact Disc (CD), einer Digital Versatile Disc (DVD) oder einer Blu-ray Disc (BD)™), einer Flashspeichervorrichtung, einer Speicherkarte und dergleichen umfassen.

[0112] Während die vorliegende Erfindung unter Bezugnahme auf beispielhafte Ausführungsbeispiele beschrieben wurde, ist es selbstverständlich, dass die Erfindung nicht auf die offenbarten beispielhaften Ausführungsbeispiele beschränkt ist. Es wird von dem Fachmann anerkannt werden, dass verschiedene Änderungen und Modifikationen vorgenommen werden können, ohne den Umfang der Erfindung zu verlassen, wie er durch die beigefügten Patentansprüche definiert wird. All der Merkmale, die in dieser Schrift (einschließlich jeglicher begleitender Patentansprüche, Zusammenfassung und Zeichnungen) offenbart sind, und/oder all der Schritte von jeglichem Verfahren oder Prozess, die so offenbart sind, können in jeder beliebigen Kombination kombiniert werden, mit der Ausnahme von Kombinationen, bei denen sich zumindest einige dieser Merkmale und/oder Schritte gegenseitig ausschließen.

[0113] Eine Informationsverarbeitungsvorrichtung erzeugt ein öffentliches Schlüsselpaar gemäß einer Zertifikatsausstellungsanforderung, erzeugt eine Zertifikatssignierungsanforderung basierend auf dem öffentlichen Schlüsselpaar und überträgt die Zertifikatssignierungsanforderung an eine externe Vorrichtung. Die Informationsverarbeitungsvorrichtung erfasst ein elektronisches Zertifikat und ein Zertifikatsausstellungsanforderungsergebnis von der externen Vorrichtung als Antwort auf die Ausstellungsanforderung und stellt die Anwendung des erfassten elektronischen Zertifikats ein.

Patentansprüche

1. Informationsverarbeitungsvorrichtung mit:
einem Erzeuger, der konfiguriert ist zum Erzeugen eines öffentlichen Schlüsselpaars und Erzeugen einer Zertifikatssignierungsanforderung basierend auf dem erzeugten öffentlichen Schlüsselpaar;
einem Sender, der konfiguriert ist zum Übertragen einer Elektronisches-Zertifikat-Ausstellungsanforderung, die die erzeugte Zertifikatssignierungsanforderung umfasst, an eine externe Vorrichtung;
einem Empfänger, der konfiguriert ist zum Empfangen einer Antwort, die von der externen Vorrichtung als Antwort auf die Elektronisches-Zertifikat-Ausstellungsanforderung übertragen wird;
einer ersten Erfassungseinheit, die konfiguriert ist zum Erfassen eines elektronischen Zertifikats, das in der durch den Empfänger empfangenen Antwort umfasst ist; und
einem Prozessor, der konfiguriert ist zum Bewirken, dass eine Anwendung ihre Verwendung des elektronischen Zertifikats ermöglicht, das durch die erste Erfassungseinheit erfasst wird.

2. Vorrichtung gemäß Anspruch 1, zusätzlich mit:
einer Verifizierungseinheit, die konfiguriert ist zum Authentisieren einer in der empfangenen Antwort umfassten elektronischen Signatur, um zu verifizieren, ob die empfangene Antwort durch die externe Vorrichtung übertragen wurde,
wobei die erste Erfassungseinheit konfiguriert ist zum Erfassen des in der empfangenen Antwort umfassten elektronischen Zertifikats abhängig von dem Ausgang der Authentisierung durch die Verifizierungseinheit.

3. Vorrichtung gemäß Anspruch 2, zusätzlich mit:
einer zweiten Erfassungseinheit, die konfiguriert ist zum Erfassen eines CA-Zertifikats von der externen Vorrichtung,
wobei die Verifizierungseinheit konfiguriert ist zum Durchführen der Authentisierung der elektronischen Signatur unter Verwendung des durch die zweite Erfassungseinheit erfassten CA-Zertifikats.

4. Vorrichtung gemäß einem der Ansprüche 1 bis 3, wobei der Empfänger konfiguriert ist zum Empfangen einer Anweisung für die Übertragung der Elektronisches-Zertifikat-Ausstellungsanforderung von einer zweiten Informationsverarbeitungsvorrichtung, die mit der Informationsverarbeitungsvorrichtung über ein Kommunikationsnetzwerk verbunden ist.

5. Vorrichtung gemäß Anspruch 4, wobei:
der Prozessor konfiguriert ist zum Erzeugen von Anzeigesteuerdaten zum Anzeigen einer ersten Benutzerschnittstelle zum Annehmen einer Benutzereingabe; und
der Sender konfiguriert ist zum Übertragen der erzeugten Anzeigesteuerdaten an die zweite Informationsverarbeitungsvorrichtung, um zu bewirken, dass die zweite Informationsverarbeitungsvorrichtung die erste Benutzerschnittstelle anzeigt,
wobei die Anweisung für die Übertragung der Elektronisches-Zertifikat-Ausstellungsanforderung durch die zweite Informationsverarbeitungsvorrichtung gemäß der Benutzereingabe übertragen wird, die über die

angezeigte erste Benutzerschnittstelle angenommen wird.

6. Vorrichtung gemäß einem der vorhergehenden Ansprüche, wobei der Prozessor konfiguriert ist zum:
Erzeugen von Verbindungseinrichtungsanzeigedaten zum Anzeigen einer zweiten Benutzerschnittstelle zum Annehmen einer Benutzereingabe;
Bewirken, dass die zweite Benutzerschnittstelle angezeigt wird, sodass die Benutzereingabe über die zweite Benutzerschnittstelle angenommen werden kann; und
Bewirken, dass eine Verbindung mit der externen Vorrichtung gemäß der angenommenen Benutzereingabe hergestellt wird,
wobei der Sender die Elektronisches-Zertifikat-Ausstellungsanforderung an die externe Vorrichtung überträgt, mit der die Verbindung hergestellt wurde.

7. Vorrichtung gemäß einem der vorhergehenden Ansprüche, wobei:
der Prozessor konfiguriert ist zum Bewirken, dass die Informationsverarbeitungsvorrichtung das elektronische Zertifikat in der Anwendung verwendet.

8. Vorrichtung gemäß einem der vorhergehenden Ansprüche, zusätzlich mit einer Aktualisierungseinheit, die konfiguriert ist zum:
Einstellen einer Aktualisierungszeit zum Aktualisieren des elektronischen Zertifikats; und
Aktualisieren des elektronischen Zertifikats zu der eingestellten Aktualisierungszeit durch Aktivieren des Senders, des Empfängers und der ersten Erfassungseinheit zum Übertragen der Elektronisches-Zertifikat-Ausstellungsanforderung und Erfassen eines zweiten elektronischen Zertifikats.

9. Vorrichtung gemäß Anspruch 8, wobei die Aktualisierungseinheit konfiguriert ist zum Einstellen der Aktualisierungszeit basierend auf zumindest einem von: einem Datum und einer Zeit; einer Anzahl von Tagen, die eine Zeitdauer vor einem Ablauf des elektronischen Zertifikats definiert; und einem Aktualisierungszyklus.

10. Verfahren zur Steuerung einer Informationsverarbeitungsvorrichtung, die konfiguriert ist zum Durchführen einer Kommunikation unter Verwendung eines elektronischen Zertifikats, wobei das Verfahren aufweist:
Erzeugen eines öffentlichen Schlüsselpaars und Erzeugen einer Zertifikatssignierungsanforderung basierend auf dem erzeugten öffentlichen Schlüsselpaar;
Übertragen einer Elektronisches-Zertifikat-Ausstellungsanforderung, die die erzeugte Zertifikatssignierungsanforderung umfasst, an eine externe Vorrichtung;
Empfangen einer Antwort, die von der externen Vorrichtung als Antwort auf die Elektronisches-Zertifikat-Ausstellungsanforderung übertragen wird;
Erfassen eines elektronischen Zertifikats, das in der beim Empfangen empfangenen Antwort umfasst ist; und
Bewirken, dass eine Anwendung ihre Verwendung des elektronischen Zertifikats ermöglicht, das beim Erfassen erfasst wird.

11. Verfahren gemäß Anspruch 10, zusätzlich mit:
Authentisieren einer in der empfangenen Antwort umfassten elektronischen Signatur, um zu verifizieren, ob die empfangene Antwort durch die externe Vorrichtung übertragen wurde,
wobei das Erfassen des in der empfangenen Antwort umfassten elektronischen Zertifikats abhängig von dem Ausgang des Authentisierens durchgeführt wird.

12. Verfahren gemäß Anspruch 11, zusätzlich mit:
Erfassen eines CA-Zertifikats von der externen Vorrichtung,
wobei die Authentisierung der elektronischen Signatur unter Verwendung des erfassten CA-Zertifikats durchgeführt wird.

13. Verfahren gemäß einem der Ansprüche 10 bis 12, zusätzlich mit:
Empfangen einer Anweisung für die Übertragung der Elektronisches-Zertifikat-Ausstellungsanforderung von einer zweiten Informationsverarbeitungsvorrichtung, die mit der Informationsverarbeitungsvorrichtung über ein Kommunikationsnetzwerk verbunden ist.

14. Verfahren gemäß Anspruch 13, zusätzlich mit:
Erzeugen von Anzeigesteuerdaten zum Anzeigen einer ersten Benutzerschnittstelle zum Annehmen einer Benutzereingabe; und
Übertragen der erzeugten Anzeigesteuerdaten an die zweite Informationsverarbeitungsvorrichtung, um zu bewirken, dass die zweite Informationsverarbeitungsvorrichtung die erste Benutzerschnittstelle anzeigt,
wobei die Anweisung für die Übertragung der Elektronisches-Zertifikat-Ausstellungsanforderung durch die zweite Informationsverarbeitungsvorrichtung gemäß der Benutzereingabe übertragen wird, die über die angezeigte erste Benutzerschnittstelle angenommen wird.

15. Verfahren gemäß einem der Ansprüche 10 bis 14, zusätzlich mit:
Erzeugen von Verbindungseinrichtungsanzeigedaten zum Anzeigen einer zweiten Benutzerschnittstelle zum Annehmen einer Benutzereingabe;
Bewirken, dass die zweite Benutzerschnittstelle angezeigt wird, sodass die Benutzereingabe über die zweite Benutzerschnittstelle angenommen werden kann; und

Bewirken, dass eine Verbindung mit der externen Vorrichtung gemäß der angenommenen Benutzereingabe hergestellt wird,
wobei das Übertragen der Elektronisches-Zertifikat-Ausstellungsanforderung an die externe Vorrichtung erfolgt, mit der die Verbindung hergestellt wurde.

16. Verfahren gemäß einem der Ansprüche 10 bis 15, zusätzlich mit:
Bewirken, dass die Informationsverarbeitungsvorrichtung das elektronische Zertifikat in der Anwendung verwendet.

17. Verfahren gemäß einem der Ansprüche 10 bis 16, zusätzlich mit:
Einstellen einer Aktualisierungszeit zum Aktualisieren des elektronischen Zertifikats; und
Aktualisieren des elektronischen Zertifikats zu der eingestellten Aktualisierungszeit durch Durchführen des Übertragens der Elektronisches-Zertifikat-Ausstellungsanforderung und des Erfassens eines zweiten elektronischen Zertifikats.

18. Bilderzeugungsvorrichtung mit:
einer Verwaltungseinheit, die konfiguriert ist zum Verwalten eines elektronischen Zertifikats;
einer Aktualisierungsverwaltungseinheit, die konfiguriert ist zum Einstellen einer aus einer Vielzahl von Aktualisierungsregeln ausgewählten Aktualisierungsregel, die für das durch die Verwaltungseinheit verwaltete elektronische Zertifikat anwendbar ist; und einem Sender, der konfiguriert ist zum Übertragen, basierend auf der eingestellten Aktualisierungsregel, einer Elektronisches-Zertifikat-Aktualisierungsanforderung an eine externe Vorrichtung.

19. Bilderzeugungsvorrichtung gemäß Anspruch 18, zusätzlich mit der Informationsverarbeitungsvorrichtung gemäß einem der Ansprüche 1 bis 9.

20. Verfahren zur Steuerung einer Bilderzeugungsvorrichtung, die konfiguriert ist zum Durchführen einer Kommunikation unter Verwendung eines elektronischen Zertifikats, wobei das Verfahren aufweist:
Verwalten des elektronischen Zertifikats;
Einstellen einer aus einer Vielzahl von Aktualisierungsregeln ausgewählten Aktualisierungsregel, die für das verwaltete elektronische Zertifikat anwendbar ist; und
Übertragen, basierend auf der eingestellten Aktualisierungsregel, einer Elektronisches-Zertifikat-Aktualisierungsanforderung an eine externe Vorrichtung.

21. Verfahren gemäß Anspruch 20, wobei die Bilderzeugungsvorrichtung zusätzlich eine Informationsverarbeitungsvorrichtung aufweist, und das Verfahren zusätzlich das Verfahren zur Steuerung der Informationsverarbeitungsvorrichtung gemäß einem der Ansprüche 10 bis 17 aufweist.

22. System mit zumindest einer Informationsverarbeitungsvorrichtung gemäß einem der Ansprüche 1 bis 9 und einer externen Vorrichtung, die aufweist:
einen Empfänger, der konfiguriert ist zum Empfangen der durch die Informationsverarbeitungsvorrichtung übertragenen Elektron isches-Zertifikat-Ausstellungsanforderung;
einen Prozessor, der konfiguriert ist zum Verarbeiten der empfangenen Elektronisches-Zertifikat-Ausstellungsanforderung, Erfassen eines elektronischen Zertifikats und Erzeugen einer Antwort, die das erfasste elektronische Zertifikat umfasst; und
einen Sender, der konfiguriert ist zum Übertragen der erzeugten Antwort an die Informationsverarbeitungsvorrichtung.

23. System gemäß Anspruch 22, wobei der Prozessor der externen Vorrichtung konfiguriert ist zum:
Einfügen einer elektronischen Signatur in die übertragene Antwort, sodass die Informationsverarbeitungsvorrichtung die Herkunft der Antwort verifizieren kann.

24. System gemäß Anspruch 23, wobei der Prozessor der externen Vorrichtung konfiguriert ist zum:
Erzeugen eines CA-Zertifikats und Bewirken, dass der Sender das erzeugte CA-Zertifikat an die Informationsverarbeitungsvorrichtung überträgt, sodass die Informationsverarbeitungsvorrichtung eine Authentisierung der elektronischen Signatur unter Verwendung des CA-Zertifikats durchführen kann.

25. System gemäß einem der Ansprüche 22 bis 24, zusätzlich mit der Bilderzeugungsvorrichtung gemäß Anspruch 18 oder 19.

26. Verfahren zur Steuerung eines Systems mit einer externen Vorrichtung und zumindest einer Informationsverarbeitungsvorrichtung, die konfiguriert ist zum Durchführen einer Kommunikation unter Verwendung eines elektronischen Zertifikats, wobei das Verfahren aufweist: das Verfahren zur Steuerung einer Informationsverarbeitungsvorrichtung gemäß einem der Ansprüche 10 bis 17 und an der externen Vorrichtung:
Empfangen der durch die Informationsverarbeitungsvorrichtung übertragenen Elektronisches-Zertifikat-Ausstellungsanforderung;
Verarbeiten der empfangenen Elektronisches-Zertifikat-Ausstellungsanforderung, Erfassen eines elektronischen Zertifikats und Erzeugen einer Antwort, die das erfasste elektronische Zertifikat umfasst; und
Übertragen der erzeugten Antwort an die Informationsverarbeitungsvorrichtung.

27. Verfahren gemäß Anspruch 26, an der externen Vorrichtung zusätzlich mit:
Einfügen einer elektronischen Signatur in die übertragene Antwort, sodass die Informationsverarbei-

tungsvorrichtung die Herkunft der Antwort verifizieren kann.

28. Verfahren gemäß Anspruch 27, an der externen Vorrichtung zusätzlich mit:
Erzeugen eines CA-Zertifikats und Bewirken eines Übertragens des erzeugten CA-Zertifikats an die Informationsverarbeitungsvorrichtung, sodass die Informationsverarbeitungsvorrichtung eine Authentisierung der elektronischen Signatur unter Verwendung des CA-Zertifikats durchführen kann.

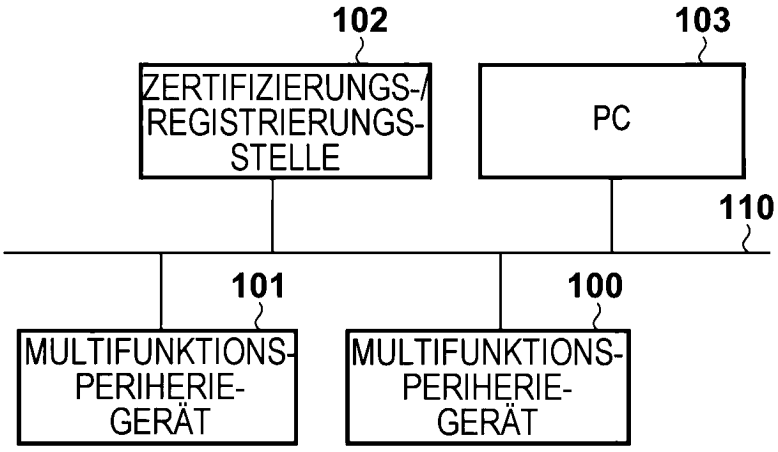
29. Verfahren gemäß einem der Ansprüche 26 bis 28, wobei das System zusätzlich eine Bilderzeugungsvorrichtung aufweist, die konfiguriert ist zum Durchführen einer Kommunikation unter Verwendung eines elektronischen Zertifikats, und das Verfahren zusätzlich das Verfahren zur Steuerung der Bilderzeugungsvorrichtung gemäß Anspruch 20 oder 21 aufweist.

30. Computerlesbares Speichermedium, das ein Programm zum Veranlassen eines Prozessors zum Betreiben eines Verfahrens gemäß einem der Ansprüche 10 bis 17, 20, 21 oder 26 bis 29 speichert.

Es folgen 21 Seiten Zeichnungen

Anhängende Zeichnungen

F I G. 1



F I G. 2

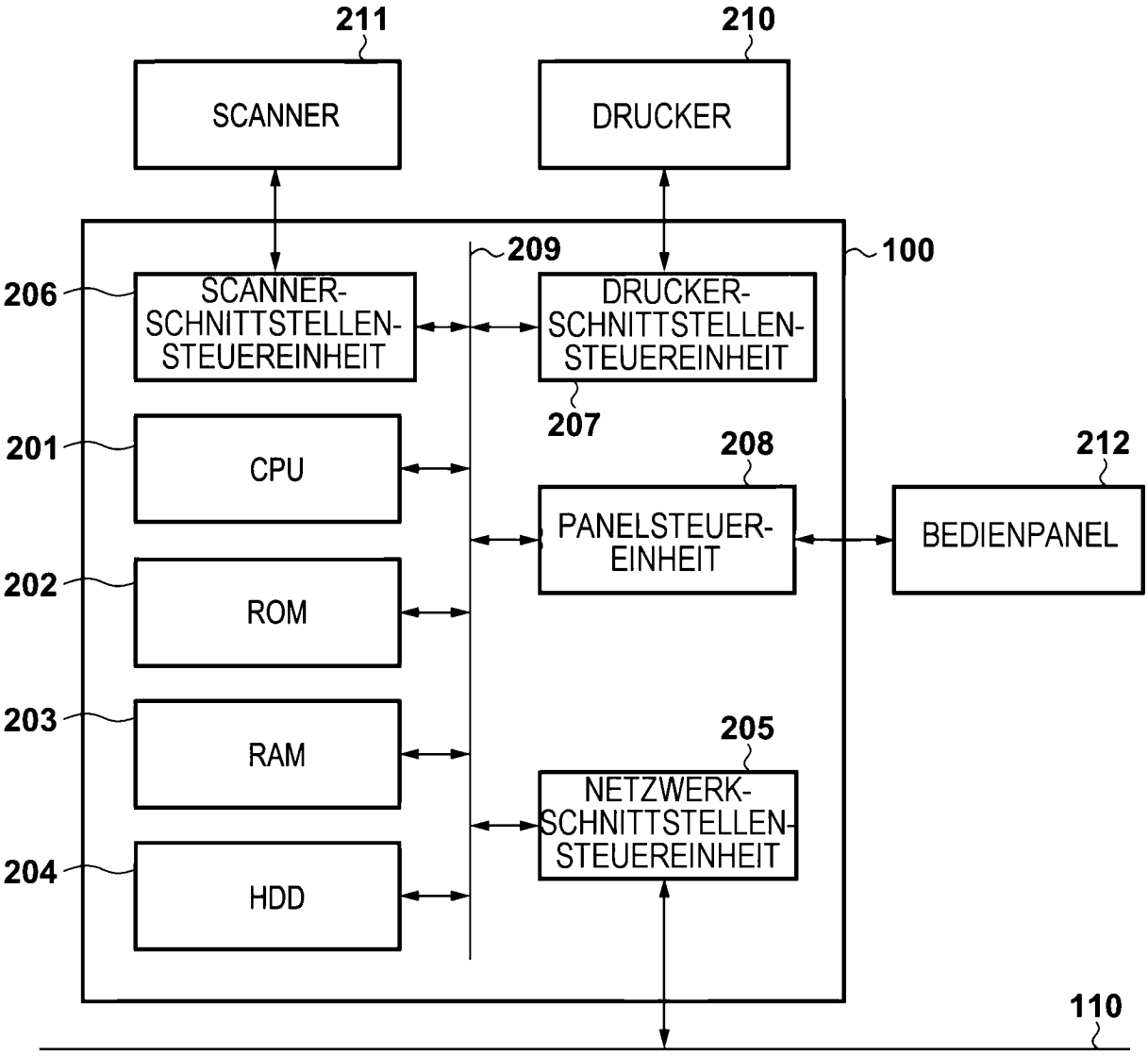


FIG. 3

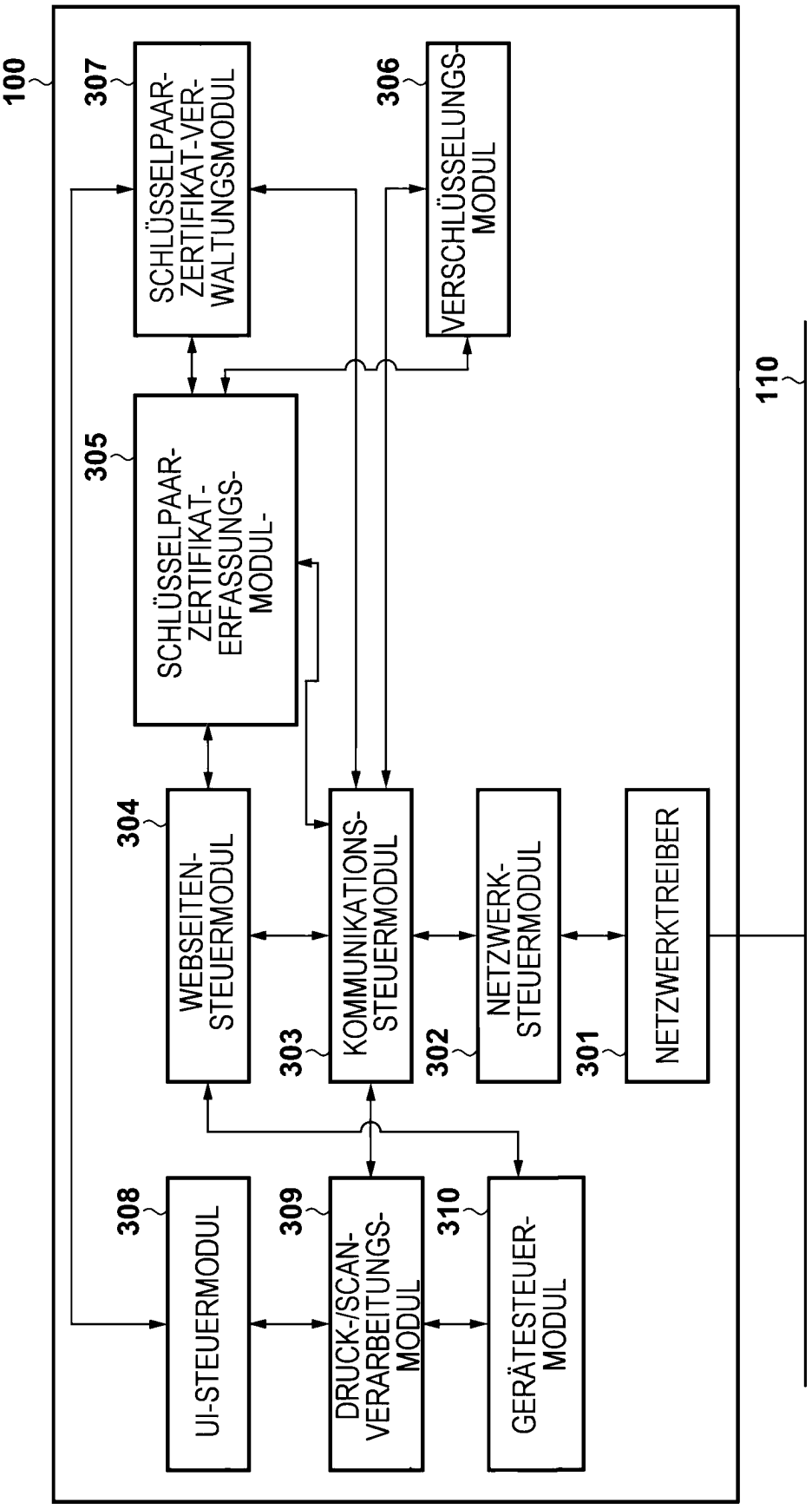

100
307
SCHLÜSSELPAAR-ZERTIFIKAT-VERWALTUNGSMODUL
306
VERSCHLÜSSELUNGS-MODUL
110
305
SCHLÜSSELPAAR-ZERTIFIKAT-ERFASSUNGS-MODUL-
304
WEBSEITEN-STEUERMODUL
303
KOMMUNIKATIONS-STEUERMODUL
302
NETZWERK-STEUERMODUL
301
NETZWERKTREIBER
308
UI-STEUERMODUL
309
DRUCK-/SCAN-VERARBEITUNGS-MODUL
310
GERÄTESTEUER-MODUL

FIG. 4A

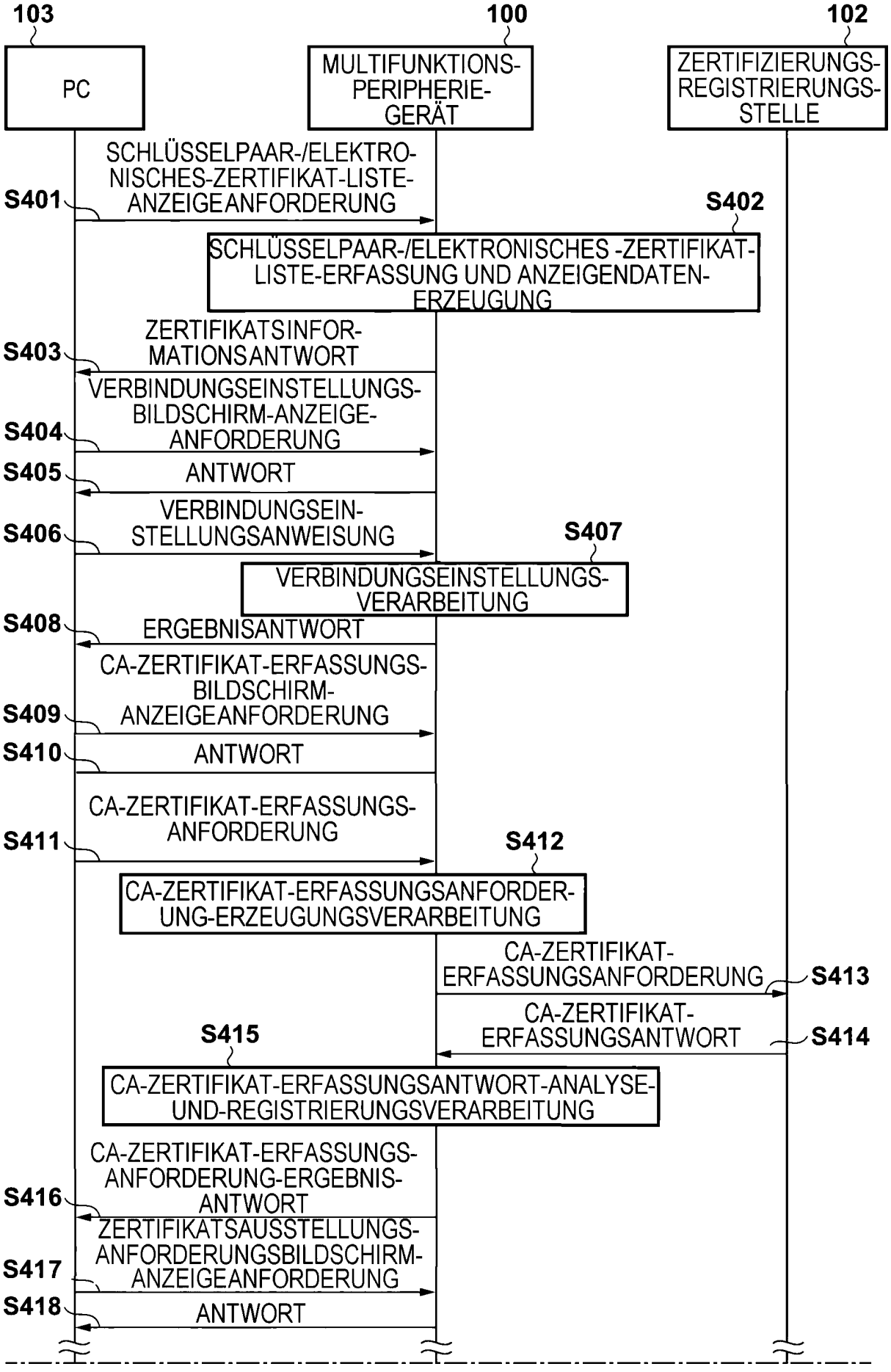

103
PC
100
MULTIFUNKTIONS-PERIPHERIE-GERÄT
102
ZERTIFIZIERUNGS-REGISTRIERUNGS-STELLE
S401
SCHLÜSSELPAAR-/ELEKTRONISCHES-ZERTIFIKAT-LISTE-ANZEIGEANFORDERUNG
S402
SCHLÜSSELPAAR-/ELEKTRONISCHES -ZERTIFIKAT-LISTE-ERFASSUNG UND ANZEIGENDATEN-ERZEUGUNG
S403
ZERTIFIKATSINFOR-MATIONSANTWORT
S404
VERBINDUNGSEINSTELLUNGS-BILDSCHIRM-ANZEIGE-ANFORDERUNG
S405
ANTWORT
S406
VERBINDUNGSEIN-STELLUNGSANWEISUNG
S407
VERBINDUNGSEINSTELLUNGS-VERARBEITUNG
S408
ERGEBNISANTWORT
S409
CA-ZERTIFIKAT-ERFASSUNGS-BILDSCHIRM-ANZEIGEANFORDERUNG
S410
ANTWORT
S411
CA-ZERTIFIKAT-ERFASSUNGS-ANFORDERUNG
S412
CA-ZERTIFIKAT-ERFASSUNGSANFORDER-UNG-ERZEUGUNGSVERARBEITUNG
CA-ZERTIFIKAT-ERFASSUNGSANFORDERUNG
S413
CA-ZERTIFIKAT-ERFASSUNGSANTWORT
S414
S415
CA-ZERTIFIKAT-ERFASSUNGSANTWORT-ANALYSE-UND-REGISTRIERUNGSVERARBEITUNG
S416
CA-ZERTIFIKAT-ERFASSUNGS-ANFORDERUNG-ERGEBNIS-ANTWORT
S417
ZERTIFIKATSAUSSTELLUNGS-ANFORDERUNGSBILDSCHIRM-ANZEIGEANFORDERUNG
S418
ANTWORT

FIG. 4B

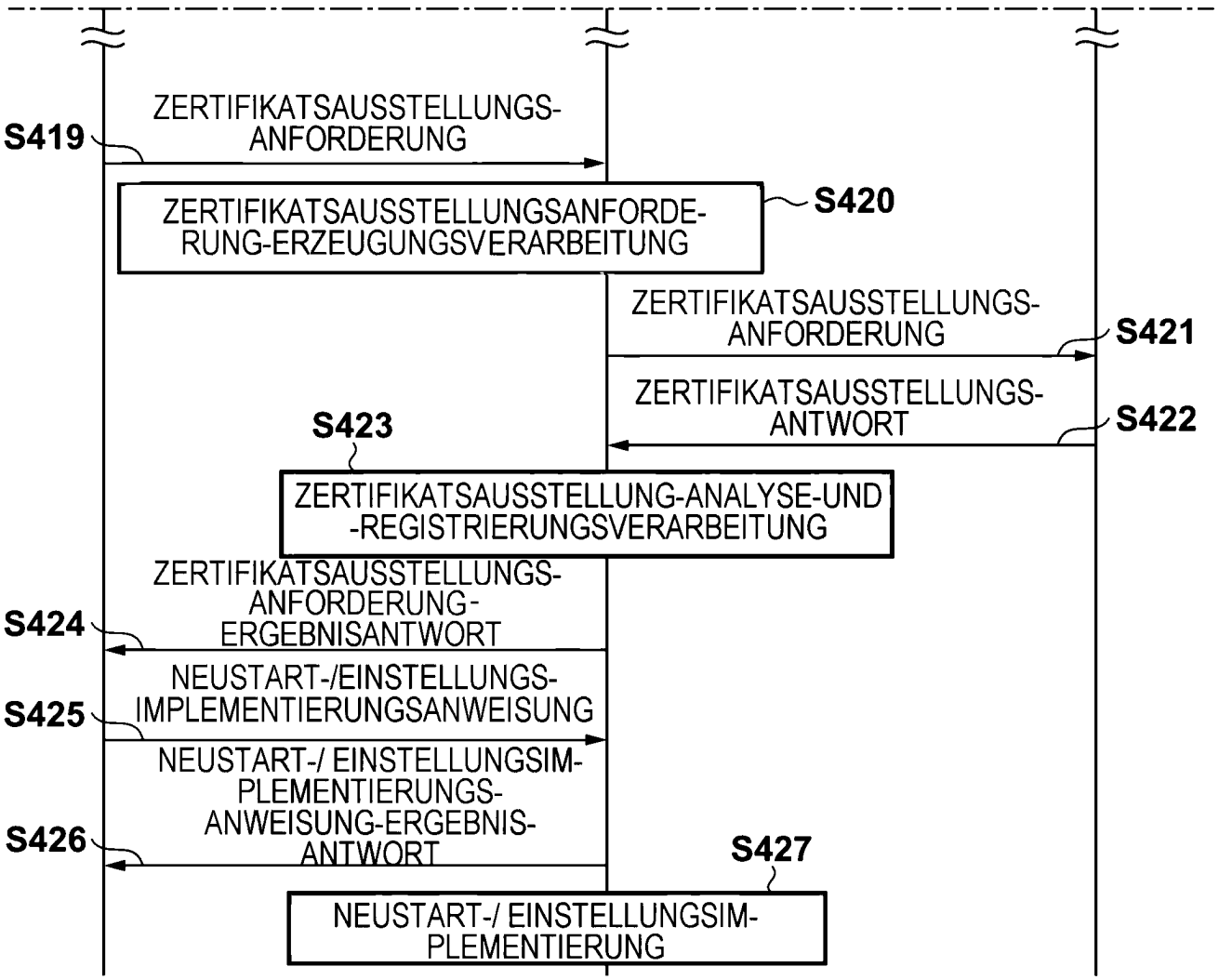

S419
ZERTIFIKATSAUSSTELLUNGS-ANFORDERUNG
ZERTIFIKATSAUSSTELLUNGSANFORDE-RUNG-ERZEUGUNGSVERARBEITUNG
S420
ZERTIFIKATSAUSSTELLUNGS-ANFORDERUNG
S421
ZERTIFIKATSAUSSTELLUNGS-ANTWORT
S422
S423
ZERTIFIKATSAUSSTELLUNG-ANALYSE-UND-REGISTRIERUNGSVERARBEITUNG
ZERTIFIKATSAUSSTELLUNGS-ANFORDERUNG-ERGEBNISANTWORT
S424
NEUSTART-/EINSTELLUNGS-IMPLEMENTIERUNGSANWEISUNG
S425
NEUSTART-/ EINSTELLUNGSIM-PLEMENTIERUNGS-ANWEISUNG-ERGEBNIS-ANTWORT
S426
S427
NEUSTART-/ EINSTELLUNGSIM-PLEMENTIERUNG

FIG. 5A

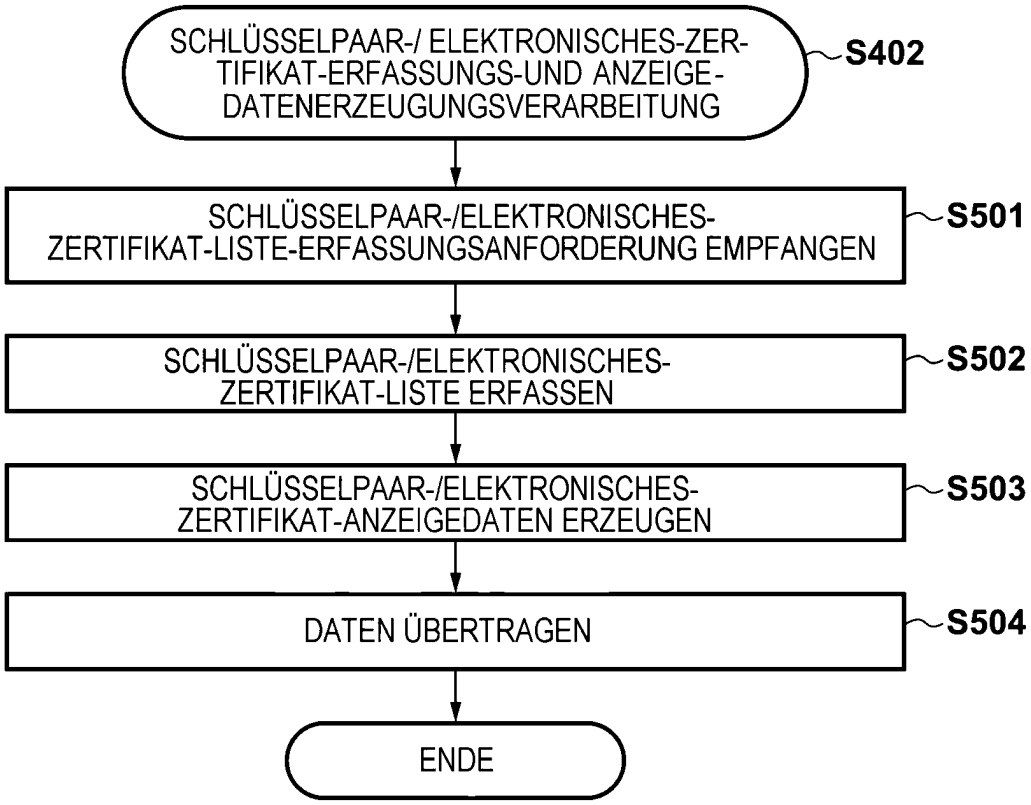

SCHLÜSSELPAAR-/ ELEKTRONISCHES-ZERTIFIKAT-ERFASSUNGS-UND ANZEIGE-DATENERZEUGUNGSVERARBEITUNG
S402
SCHLÜSSELPAAR-/ELEKTRONISCHES-ZERTIFIKAT-LISTE-ERFASSUNGSANFORDERUNG EMPFANGEN
S501
SCHLÜSSELPAAR-/ELEKTRONISCHES-ZERTIFIKAT-LISTE ERFASSEN
S502
SCHLÜSSELPAAR-/ELEKTRONISCHES-ZERTIFIKAT-ANZEIGEDATEN ERZEUGEN
S503
DATEN ÜBERTRAGEN
S504
ENDE

FIG. 5B

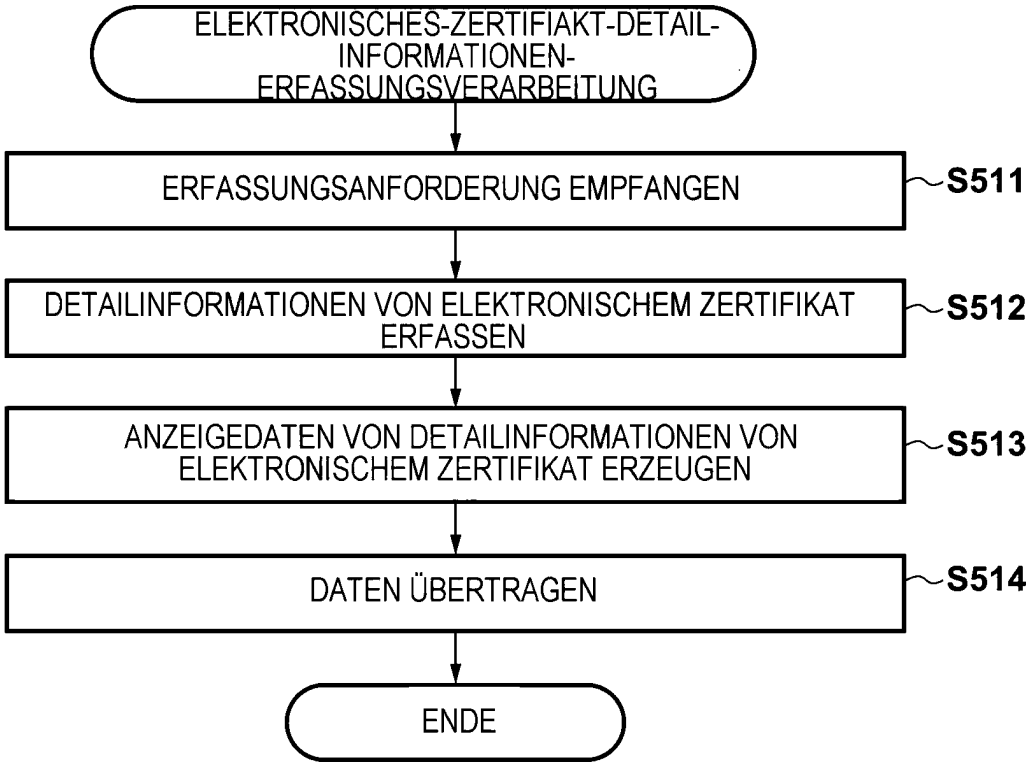
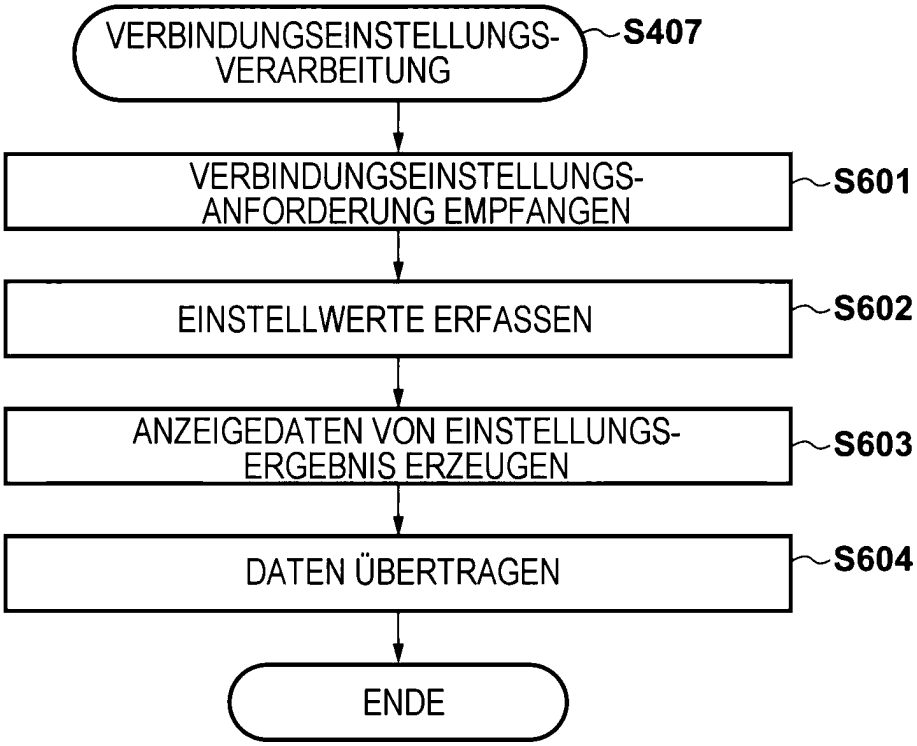

ELEKTRONISCHES-ZERTIFIAKT-DETAIL-INFORMATIONEN-ERFASSUNGSVERARBEITUNG
ERFASSUNGSANFORDERUNG EMPFANGEN
S511
DETAILINFORMATIONEN VON ELEKTRONISCHEM ZERTIFIKAT ERFASSEN
S512
ANZEIGEDATEN VON DETAILINFORMATIONEN VON ELEKTRONISCHEM ZERTIFIKAT ERZEUGEN
S513
DATEN ÜBERTRAGEN
S514
ENDE

FIG. 6


VERBINDUNGSEINSTELLUNGS-VERARBEITUNG
S407
VERBINDUNGSEINSTELLUNGS-ANFORDERUNG EMPFANGEN
S601
EINSTELLWERTE ERFASSEN
S602
ANZEIGEDATEN VON EINSTELLUNGS-ERGEBNIS ERZEUGEN
S603
DATEN ÜBERTRAGEN
S604
ENDE

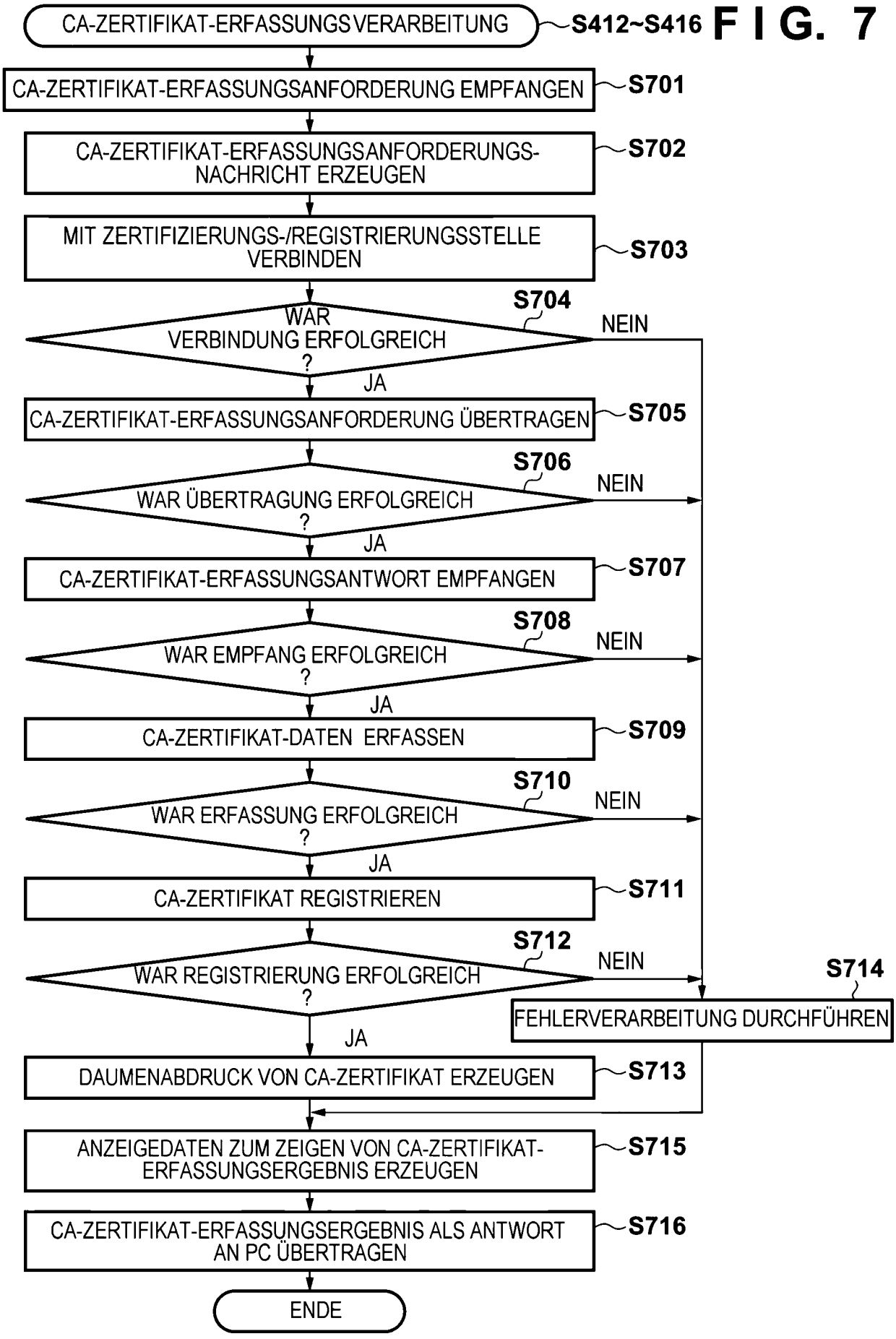

CA-ZERTIFIKAT-ERFASSUNGSVERARBEITUNG
S412~S416
CA-ZERTIFIKAT-ERFASSUNGSANFORDERUNG EMPFANGEN
S701
CA-ZERTIFIKAT-ERFASSUNGSANFORDERUNGS-NACHRICHT ERZEUGEN
S702
MIT ZERTIFIZIERUNGS-/REGISTRIERUNGSSTELLE VERBINDEN
S703
S704
WAR VERBINDUNG ERFOLGREICH ?
NEIN
JA
CA-ZERTIFIKAT-ERFASSUNGSANFORDERUNG ÜBERTRAGEN
S705
S706
WAR ÜBERTRAGUNG ERFOLGREICH ?
NEIN
JA
CA-ZERTIFIKAT-ERFASSUNGSANTWORT EMPFANGEN
S707
S708
WAR EMPFANG ERFOLGREICH ?
NEIN
JA
CA-ZERTIFIKAT-DATEN ERFASSEN
S709
S710
WAR ERFASSUNG ERFOLGREICH ?
NEIN
JA
CA-ZERTIFIKAT REGISTRIEREN
S711
S712
WAR REGISTRIERUNG ERFOLGREICH ?
NEIN
JA
S714
FEHLERVERARBEITUNG DURCHFÜHREN
DAUMENABDRUCK VON CA-ZERTIFIKAT ERZEUGEN
S713
ANZEIGEDATEN ZUM ZEIGEN VON CA-ZERTIFIKAT-ERFASSUNGSERGEBNIS ERZEUGEN
S715
CA-ZERTIFIKAT-ERFASSUNGSERGEBNIS ALS ANTWORT AN PC ÜBERTRAGEN
S716
ENDE

FIG. 7

FIG. 8A

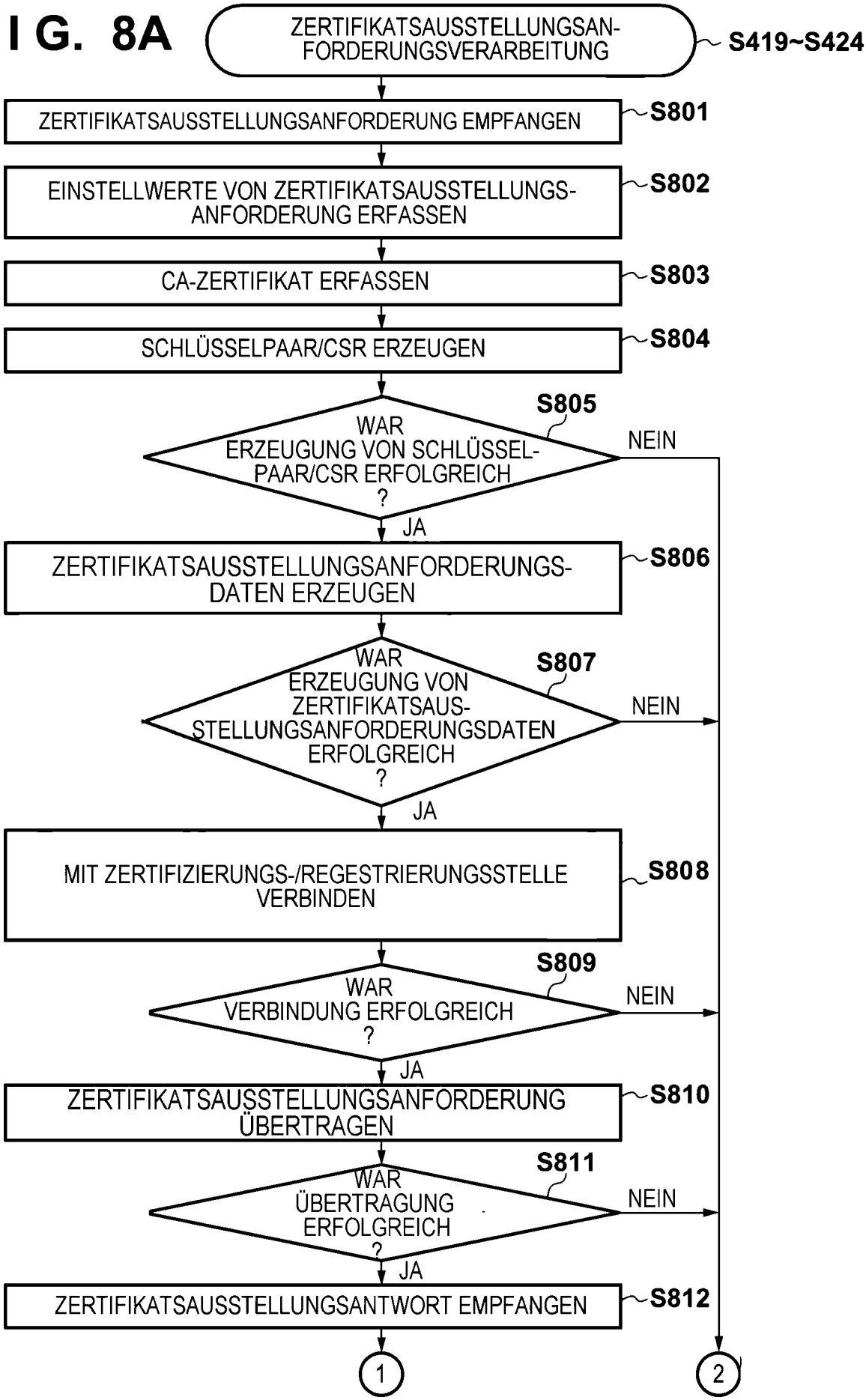

ZERTIFIKATSAUSSTELLUNGSAN-FORDERUNGSVERARBEITUNG
S419~S424
ZERTIFIKATSAUSSTELLUNGSANFORDERUNG EMPFANGEN
S801
EINSTELLWERTE VON ZERTIFIKATSAUSSTELLUNGS-ANFORDERUNG ERFASSEN
S802
CA-ZERTIFIKAT ERFASSEN
S803
SCHLÜSSELPAAR/CSR ERZEUGEN
S804
S805
WAR ERZEUGUNG VON SCHLÜSSEL-PAAR/CSR ERFOLGREICH ?
NEIN
JA
ZERTIFIKATSAUSSTELLUNGSANFORDERUNGS-DATEN ERZEUGEN
S806
S807
WAR ERZEUGUNG VON ZERTIFIKATSAUS-STELLUNGSANFORDERUNGSDATEN ERFOLGREICH ?
NEIN
JA
MIT ZERTIFIZIERUNGS-/REGESTRIERUNGSSTELLE VERBINDEN
S808
S809
WAR VERBINDUNG ERFOLGREICH ?
NEIN
JA
ZERTIFIKATSAUSSTELLUNGSANFORDERUNG ÜBERTRAGEN
S810
S811
WAR ÜBERTRAGUNG ERFOLGREICH ?
NEIN
JA
ZERTIFIKATSAUSSTELLUNGSANTWORT EMPFANGEN
S812
1
2

FIG. 8B

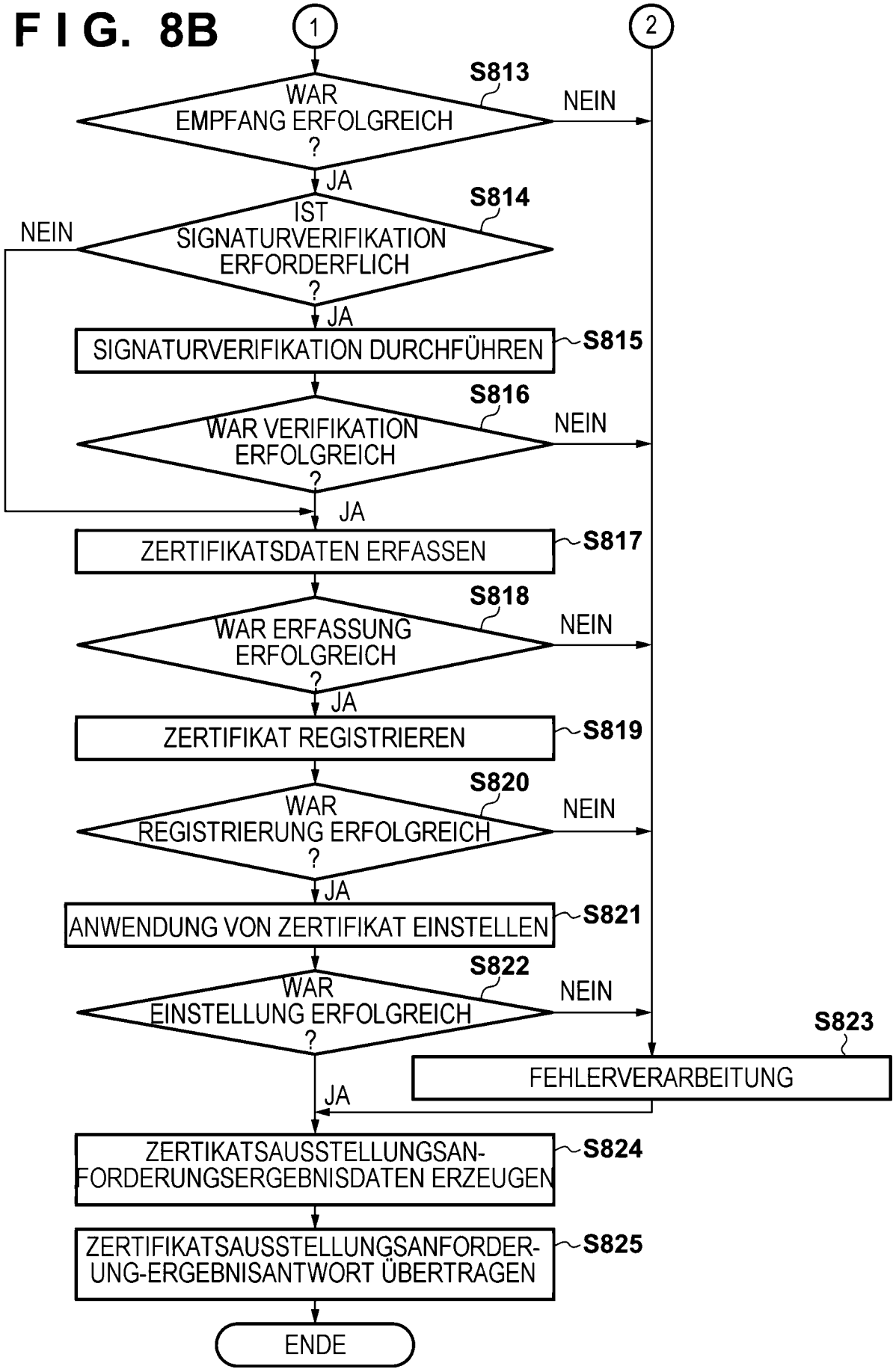

1
2
S813
WAR EMPFANG ERFOLGREICH ?
NEIN
JA
S814
IST SIGNATURVERIFIKATION ERFORDERFLICH ?
NEIN
JA
SIGNATURVERIFIKATION DURCHFÜHREN
S815
S816
WAR VERIFIKATION ERFOLGREICH ?
NEIN
JA
ZERTIFIKATSDATEN ERFASSEN
S817
S818
WAR ERFASSUNG ERFOLGREICH ?
NEIN
JA
ZERTIFIKAT REGISTRIEREN
S819
S820
WAR REGISTRIERUNG ERFOLGREICH ?
NEIN
JA
ANWENDUNG VON ZERTIFIKAT EINSTELLEN
S821
S822
WAR EINSTELLUNG ERFOLGREICH ?
NEIN
JA
S823
FEHLERVERARBEITUNG
ZERTIKATSAUSSTELLUNGSAN-FORDERUNGSERGEBNISDATEN ERZEUGEN
S824
ZERTIFIKATSAUSSTELLUNGSANFORDER-UNG-ERGEBNISANTWORT ÜBERTRAGEN
S825
ENDE

FIG. 9

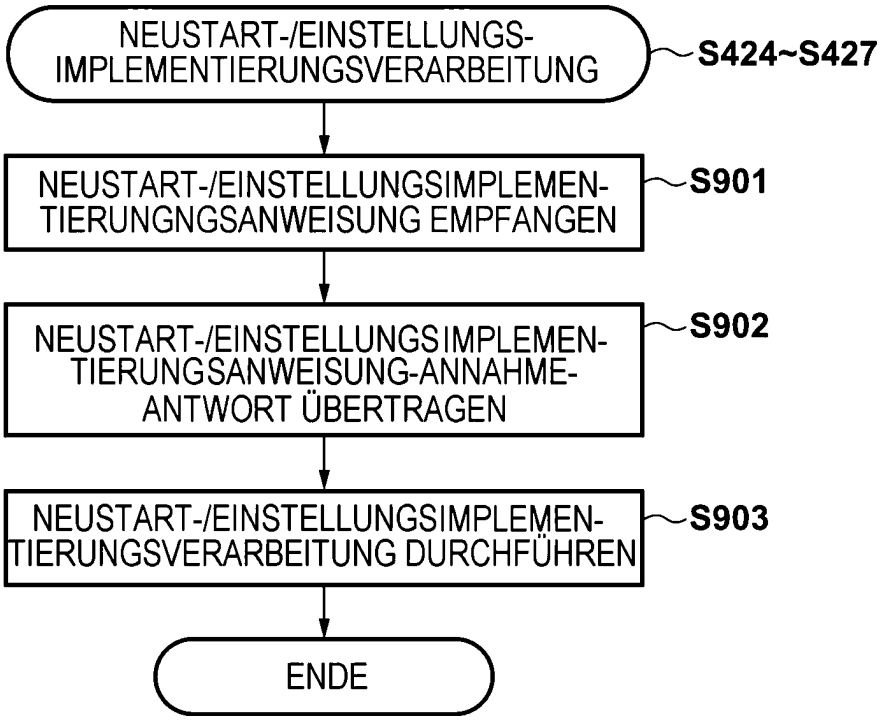

NEUSTART-/EINSTELLUNGS-IMPLEMENTIERUNGSVERARBEITUNG
S424~S427
NEUSTART-/EINSTELLUNGSIMPLEMENTIERUNGNGSANWEISUNG EMPFANGEN
S901
NEUSTART-/EINSTELLUNGSIMPLEMENTIERUNGSANWEISUNG-ANNAHME-ANTWORT ÜBERTRAGEN
S902
NEUSTART-/EINSTELLUNGSIMPLEMENTIERUNGSVERARBEITUNG DURCHFÜHREN
S903
ENDE

FIG. 10A

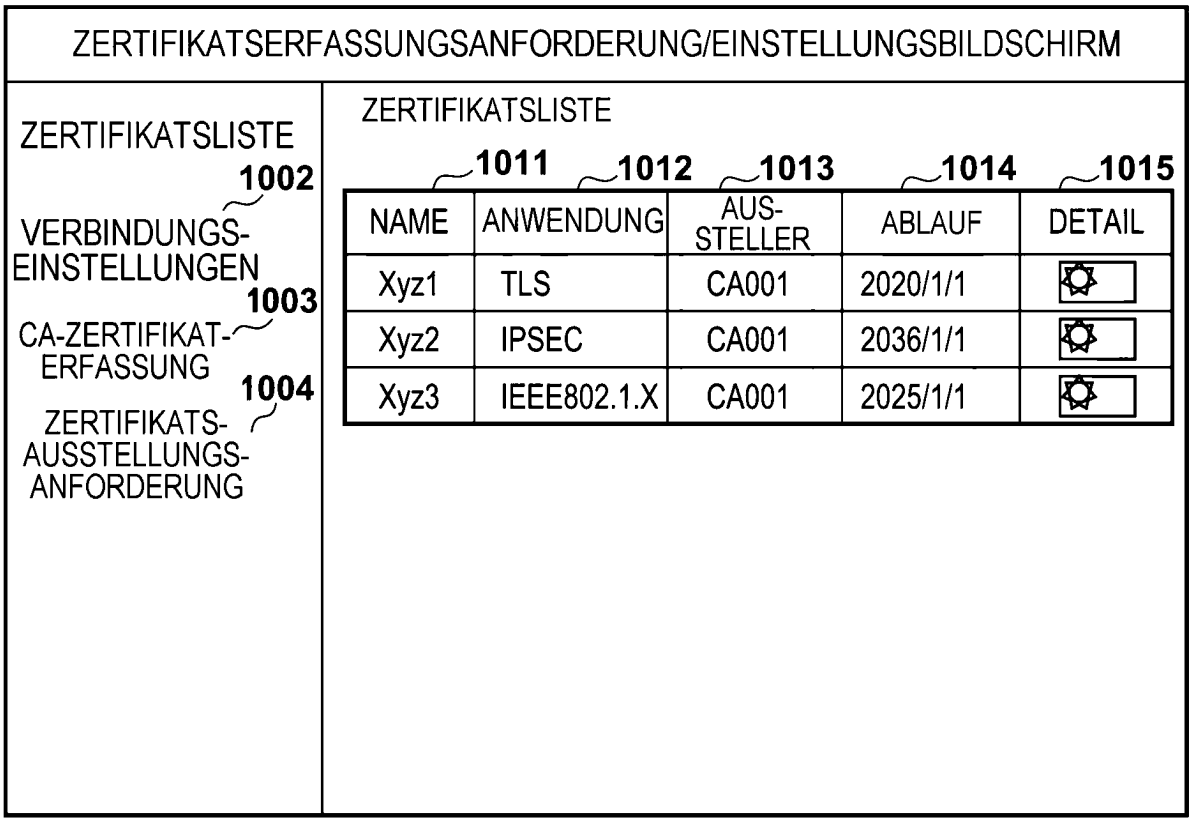


FIG. 10B

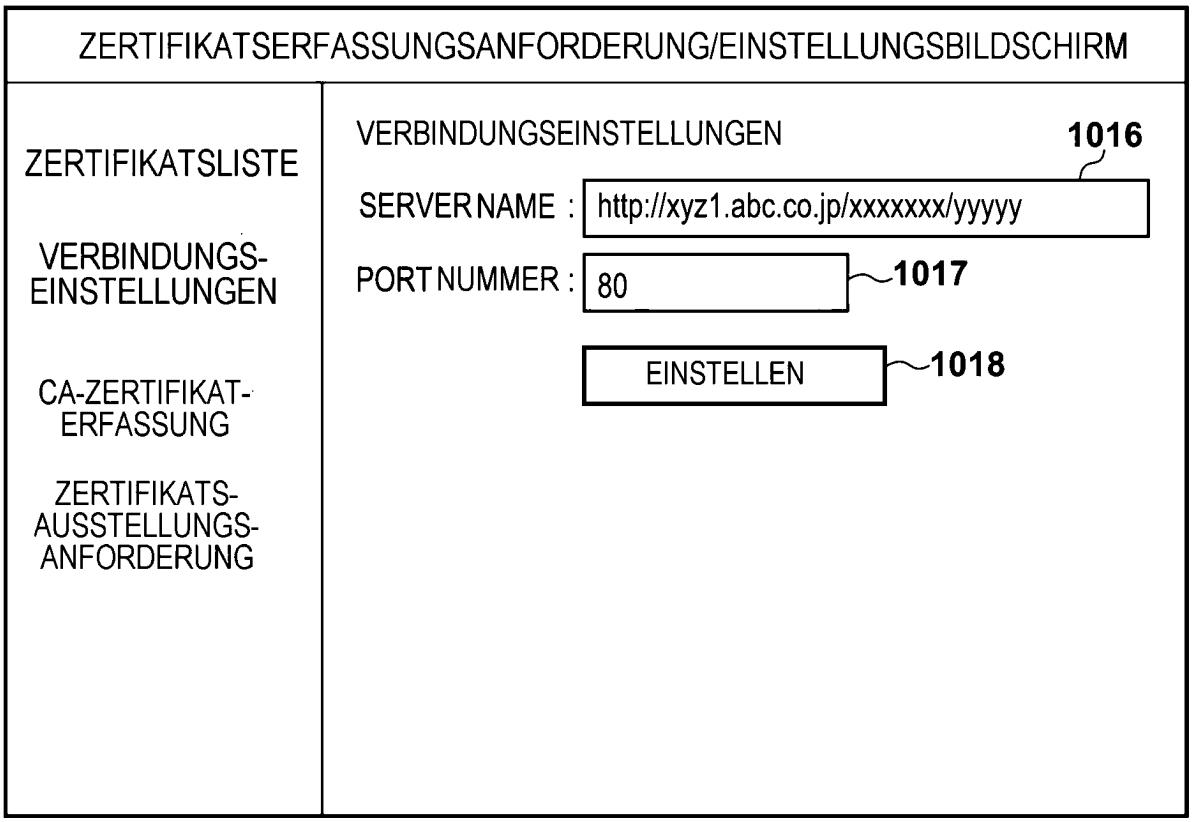


FIG. 11A

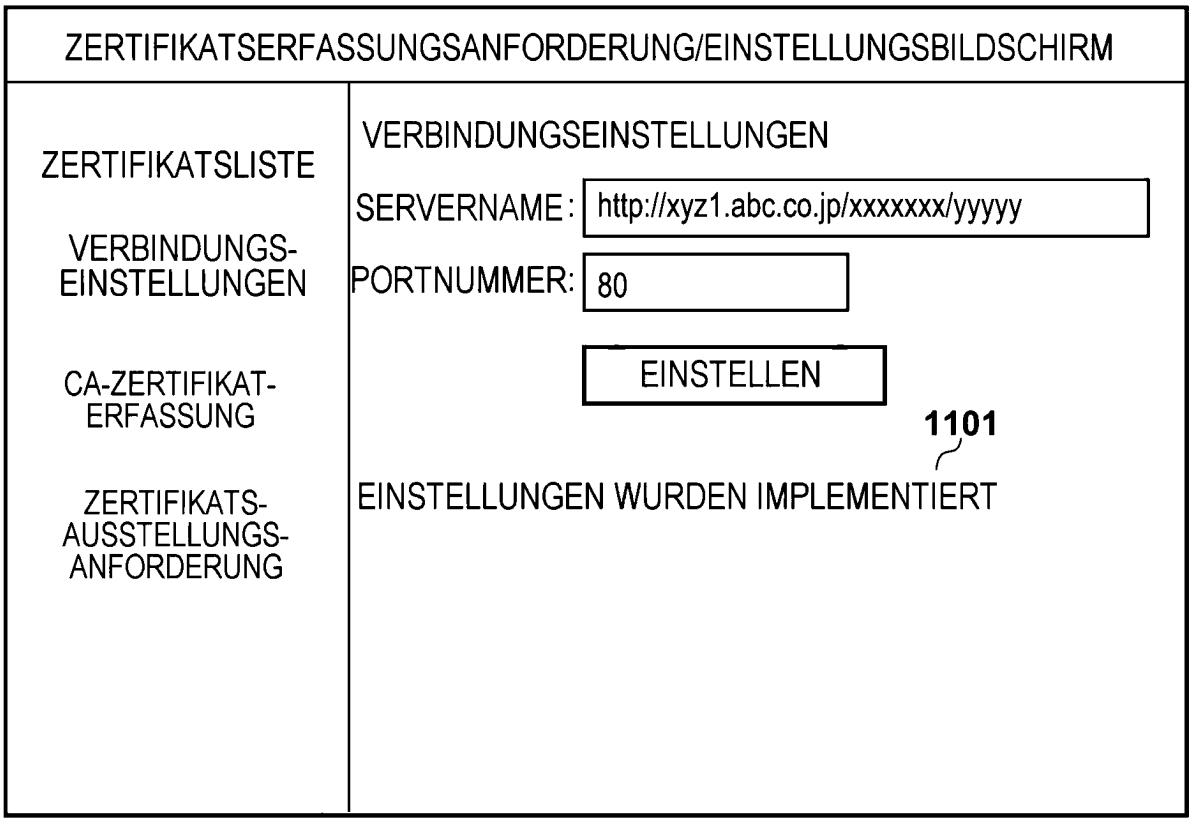
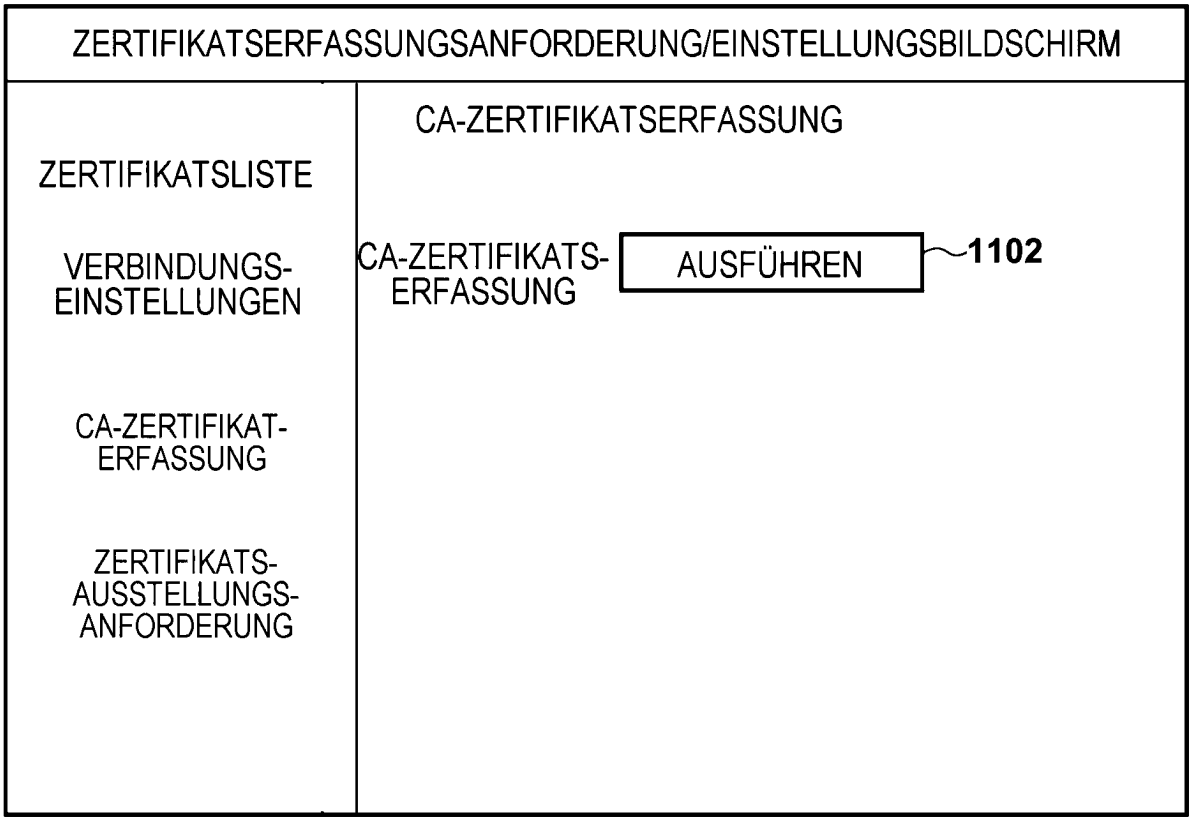
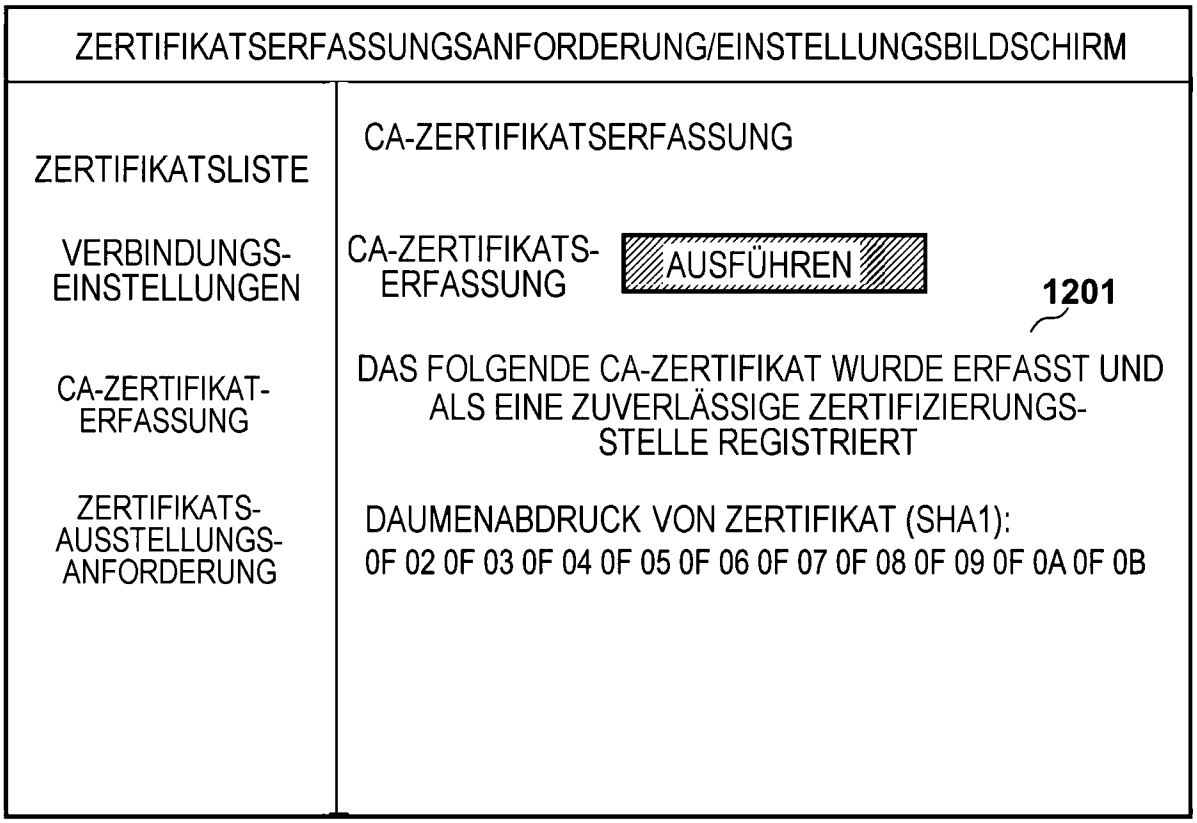


FIG. 11B



F I G. 12A



F I G. 12B

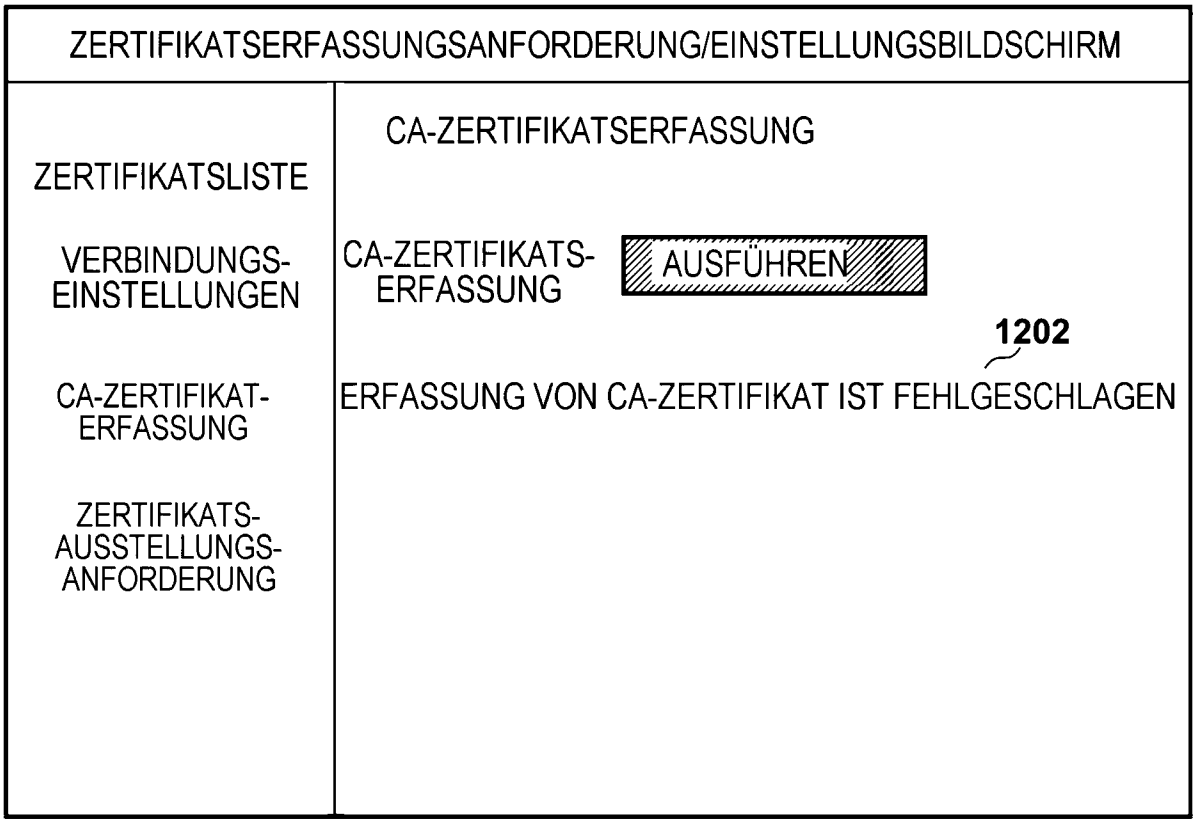


FIG. 13A

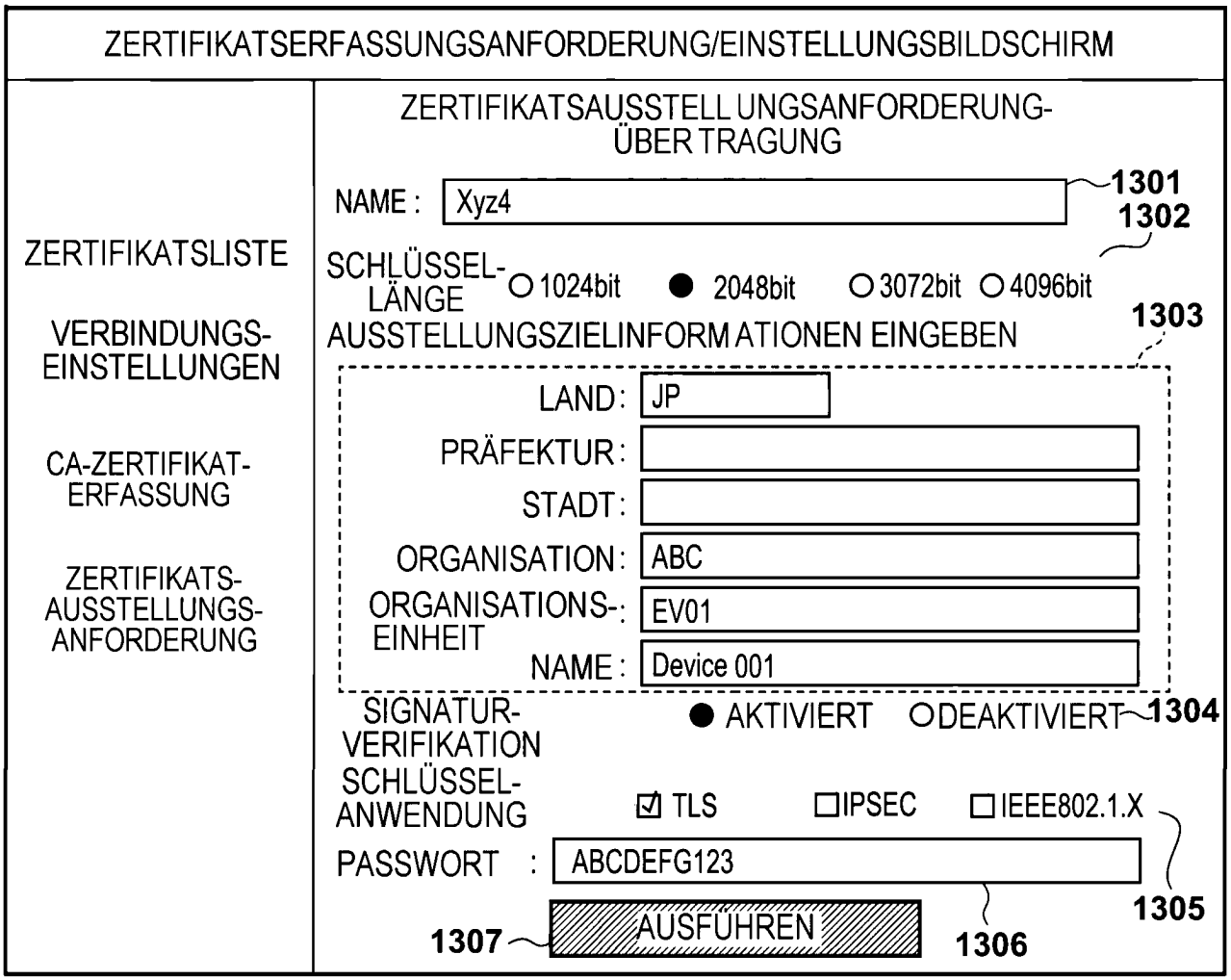


FIG. 13B

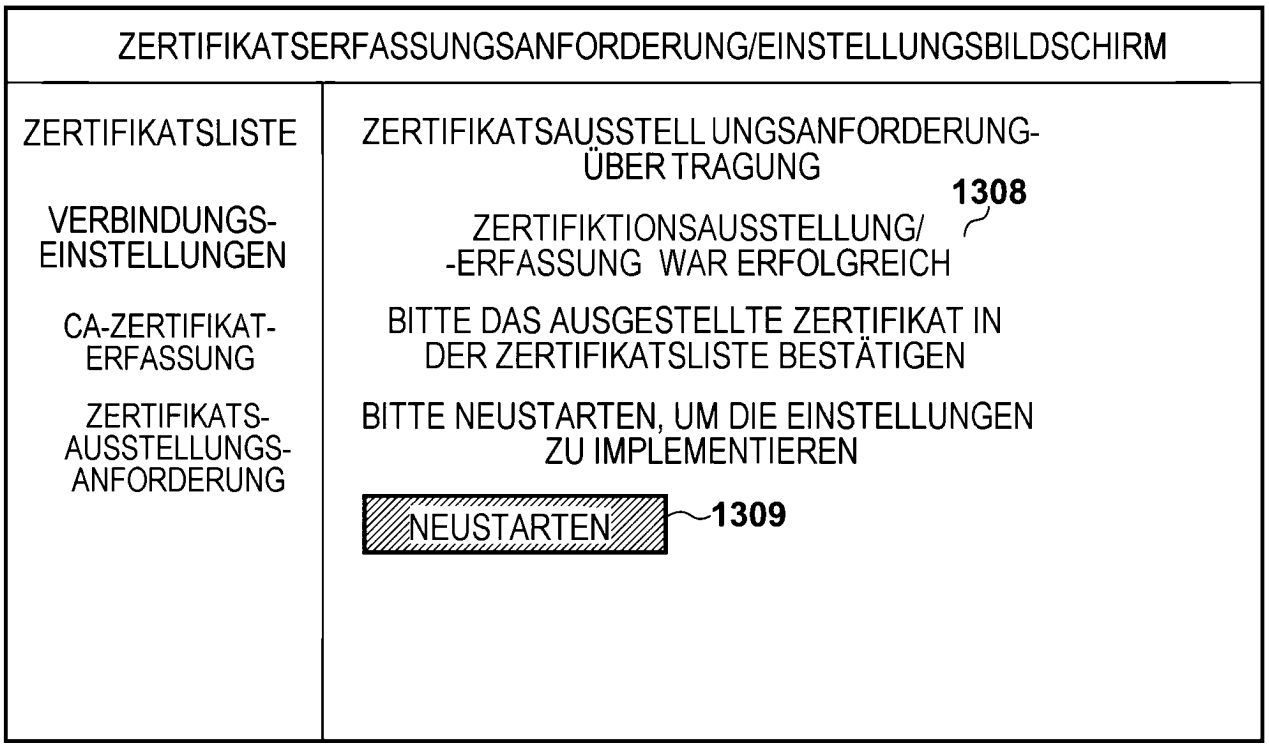


FIG. 14A

ZERTIFIKATSERFASSUNGSANFORDERUNG/EINSTELLUNGSBILDSCHIRM	
ZERTIFIKATSLISTE	ZERTIFIKATSAUSSTELLUNGSANFORDERUNG-ÜBERTRAGUNG
VERBINDUNGS-EINSTELLUNGEN	ZERTIFIKATSAUSSTELLUNG/-ERFASSUNG IST FEHLGESCHLAGEN 1401
CA-ZERTIFIKAT-ERFASSUNG	
ZERTIFIKATS-AUSSTELLUNGS-ANFORDERUNG	

FIG. 14B

ZERTIFIKATSERFASSUNGSANFORDERUNG/EINSTELLUNGSBILDSCHIRM	
ZERTIFIKATSLISTE	NEUSTART WIRD DURCHGEFÜHRT, UM DIE EINSTELLUNGEN ZU IMPLEMENTIEREN
VERBINDUNGS-EINSTELLUNGEN	
CA-ZERTIFIKAT-ERFASSUNG	
ZERTIFIKATS-AUSSTELLUNGS-ANFORDERUNG	

FIG. 15

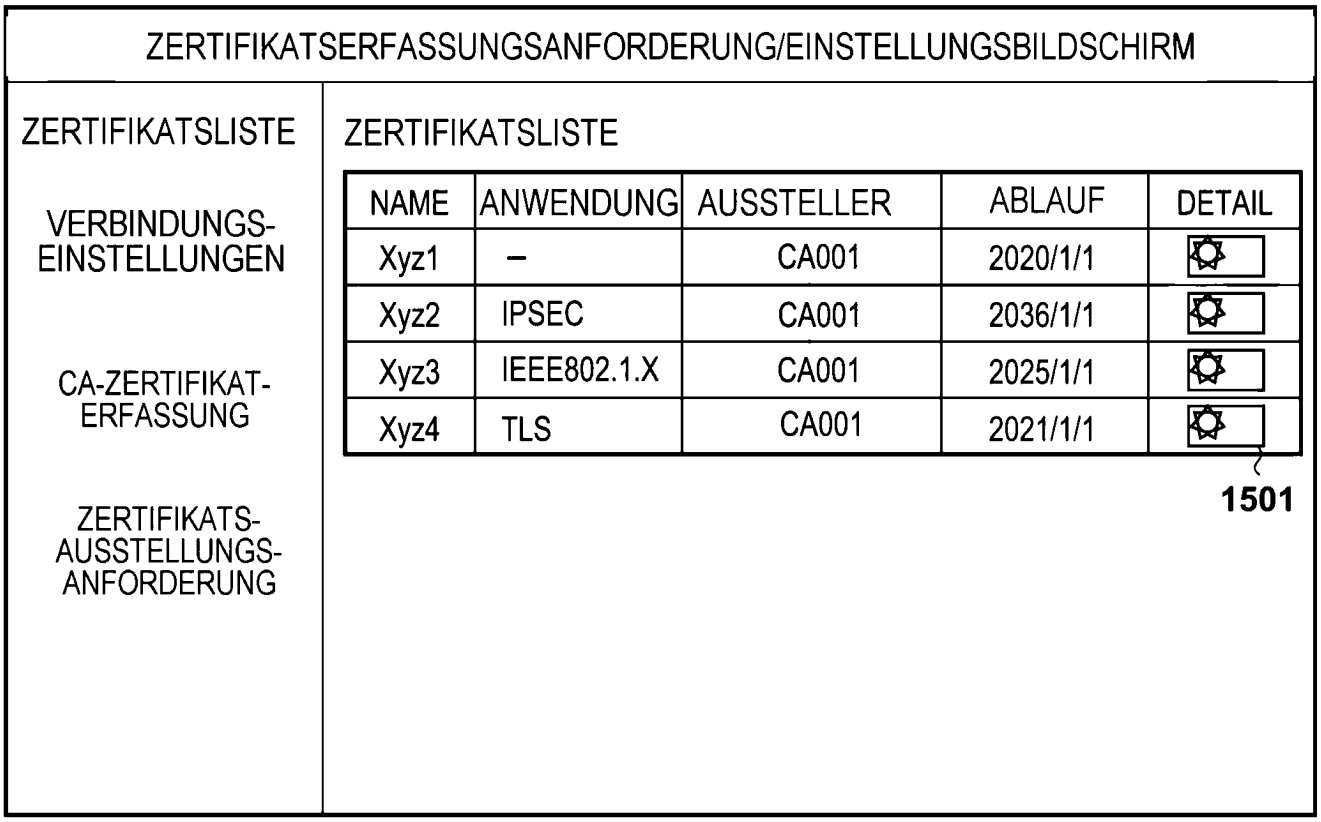

ZERTIFIKATSERFASSUNGSANFORDERUNG/EINSTELLUNGSBILDSCHIRM
ZERTIFIKATSLISTE
VERBINDUNGS-EINSTELLUNGEN
CA-ZERTIFIKAT-ERFASSUNG
ZERTIFIKATS-AUSSTELLUNGS-ANFORDERUNG
ZERTIFIKATSLISTE
NAME
ANWENDUNG
AUSSTELLER
ABLAUF
DETAIL
Xyz1
–
CA001
2020/1/1
Xyz2
IPSEC
CA001
2036/1/1
Xyz3
IEEE802.1.X
CA001
2025/1/1
Xyz4
TLS
CA001
2021/1/1
1501

FIG. 16

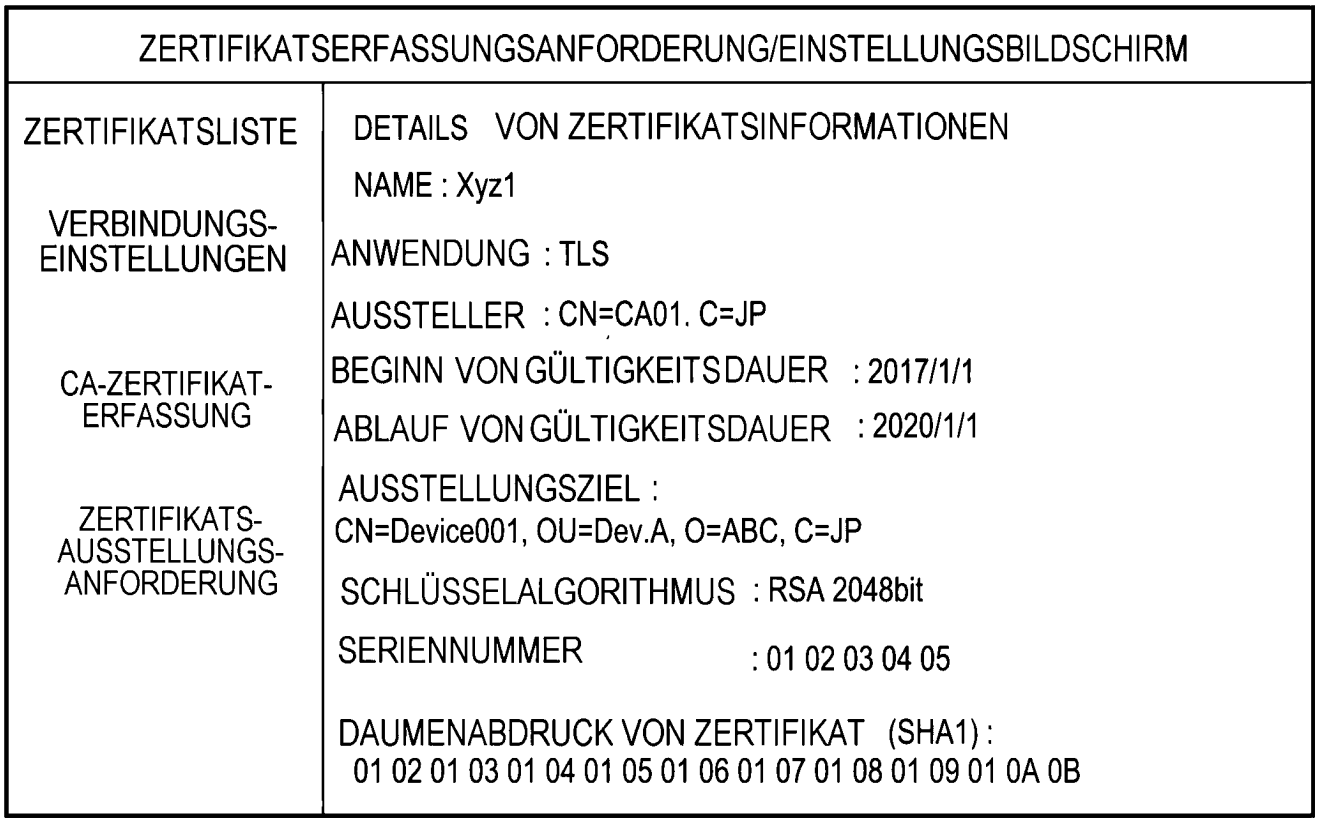

ZERTIFIKATSERFASSUNGSANFORDERUNG/EINSTELLUNGSBILDSCHIRM
ZERTIFIKATSLISTE
VERBINDUNGS-EINSTELLUNGEN
CA-ZERTIFIKAT-ERFASSUNG
ZERTIFIKATS-AUSSTELLUNGS-ANFORDERUNG
DETAILS VON ZERTIFIKATSINFORMATIONEN
NAME : Xyz1
ANWENDUNG : TLS
AUSSTELLER : CN=CA01. C=JP
BEGINN VON GÜLTIGKEITSDAUER : 2017/1/1
ABLAUF VON GÜLTIGKEITSDAUER : 2020/1/1
AUSSTELLUNGSZIEL :
CN=Device001, OU=Dev.A, O=ABC, C=JP
SCHLÜSSELALGORITHMUS : RSA 2048bit
SERIENNUMMER : 01 02 03 04 05
DAUMENABDRUCK VON ZERTIFIKAT (SHA1) :
01 02 01 03 01 04 01 05 01 06 01 07 01 08 01 09 01 0A 0B

FIG. 17A

NAME	ANWENDUNG	AUS-STELLER	BEGINN VON GÜLTIGKEITS-DAUER	ABLAUF VON GÜLTIG-KEITS-DAUER	AUSSTELLUNGS-ZIEL	ALGO-RITH-MUS	SCHLÜS-SEL-LÄNGE	SERIEN-NUMMER	DAUMEN-ABDRUCK
Xyz1	TLS	CN=CA01, C=JP	2019/1/1	2020/1/1	CN=Device001, OU=Dev.A, O=ABC, C=JP	RSA	1024	01 02 03 04 05	01 02 01 03 01 04 01 05 01 06 01 07 01 08 01 09 0A 01 0B
Xyz2	IPSEC	CN=CA01, C=JP	2015/1/1	2036/1/1	CN=Device001, OU=Dev.A, O=ABC, C=JP	RSA	2048	01 02 03 04 06	02 02 02 03 02 04 02 05 02 06 02 07 02 08 02 09 02 0A 02 0B
Xyz3	IEEE802.1X	CN=CA01, C=JP	2020/1/1	2025/1/1	CN=Device001, OU=Dev.A, O=ABC, C=JP	RSA	2048	01 02 03 04 07	03 02 03 03 03 04 03 05 03 06 03 07 03 08 03 09 03 0A 03 0B

FIG. 17B

NAME	ANWENDUNG	AUS-STELLER	BEGINN VON GÜLTIGKEITS-DAUER	ABLAUF VON GÜLTIGK-EITSDAUER	AUSSTELLUNGS-ZIEL	ALGO-RITH-MUS	SCHLÜS-SEL-LAGE	SERIEN-NUMMER	DAUMEN-ABDRUCK
Xyz1	TLS	CN=CA01, C=JP	2019/1/1	2020/1/1	CN=Device001, OU=Dev.A, O=ABC, C-JP	RSA	1024	01 02 03 04 05	02 02 02 03 02 04 02 05 02 06 02 07 02 08 01 09 0A 01 0B
Xyz2	IPSEC	CN=CA01, C=JP	2015/1/1	2036/1/1	CN=Device001, OU=Dev.A, O=ABC, C=JP	RSA	2048	01 02 03 04 06	02 02 02 03 02 04 02 05 02 06 02 07 02 08 02 09 02 0A 02 0B
Xyz3	IEEE802.1X	CN=CA01, C=JP	2020/1/1	2025/1/1	CN=Device001, OU=Dev.A, O=ABC, C=JP	RSA	2048	01 02 03 04 07	03 02 03 03 03 04 03 05 03 06 03 07 03 08 03 09 03 0A 03 0B
Xyz4	KEINE	CN=CA01, C=JP	2020/1/1	2025/1/1	CN=Device001, OU=Dev.A, O=ABC, C=JP	RSA	2048	01 02 03 04 08	04 02 04 03 04 04 04 05 04 06 04 07 04 08 04 09 04 0A 04 0B

FIG. 17C

NAME	ANWENDUNG	AUS-STELLER	BEGINN VON GÜLTIG-KEITS-DAUER	ABLAUF VON GÜLTIG-KEITS-DAUER	AUSSTELLUNGS-ZIEL	ALGO-RITH-MUS	SCHLÜS-SEL-LÄNGE	SERIEN-NUMMER	DAUMEN-ABDRUCK
Xyz1	KEINE	CN=CA01, C=JP	2019/1/1	2020/1/1	CN=Device001, OU=Dev.A, O=ABC, C=JP	RSA	1024	01 02 03 04 05	01 02 01 03 01 04 01 05 01 06 01 07 01 08 01 09 0A 01 0B
Xyz2	IPSEC	CN=CA01, C=JP	2015/1/1	2036/1/1	CN=Device001, OU=Dev.A, O=ABC, C=JP	RSA	2048	01 02 03 04 06	02 02 02 03 02 04 02 05 02 06 02 07 02 08 02 09 02 0A 02 0B
Xyz3	IEEE802.1X	CN=CA01, C=JP	2020/1/1	2025/1/1	CN=Device001, OU=Dev.A, O=ABC, C=JP	RSA	2048	01 02 03 04 07	03 02 03 03 03 04 03 05 03 06 03 07 03 08 03 09 03 0A 03 0B
Xyz4	TLS	CN=CA01, C=JP	2020/1/1	2025/1/1	CN=Device001, OU=Dev.A, O=ABC, C=JP	RSA	2048	01 02 03 04 08	04 02 04 03 04 04 04 05 04 06 04 07 04 08 04 09 04 0A 04 0B

FIG. 18

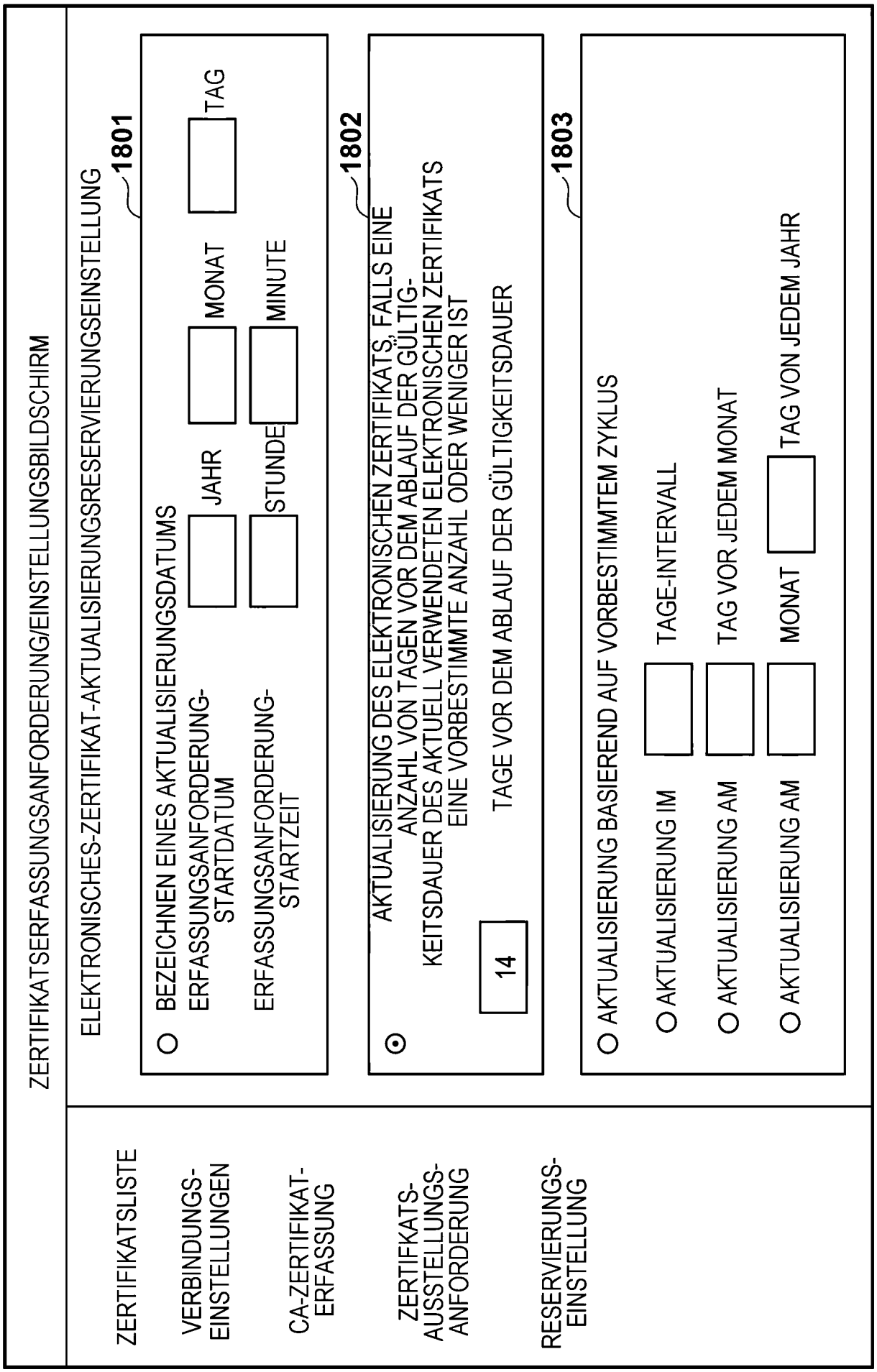
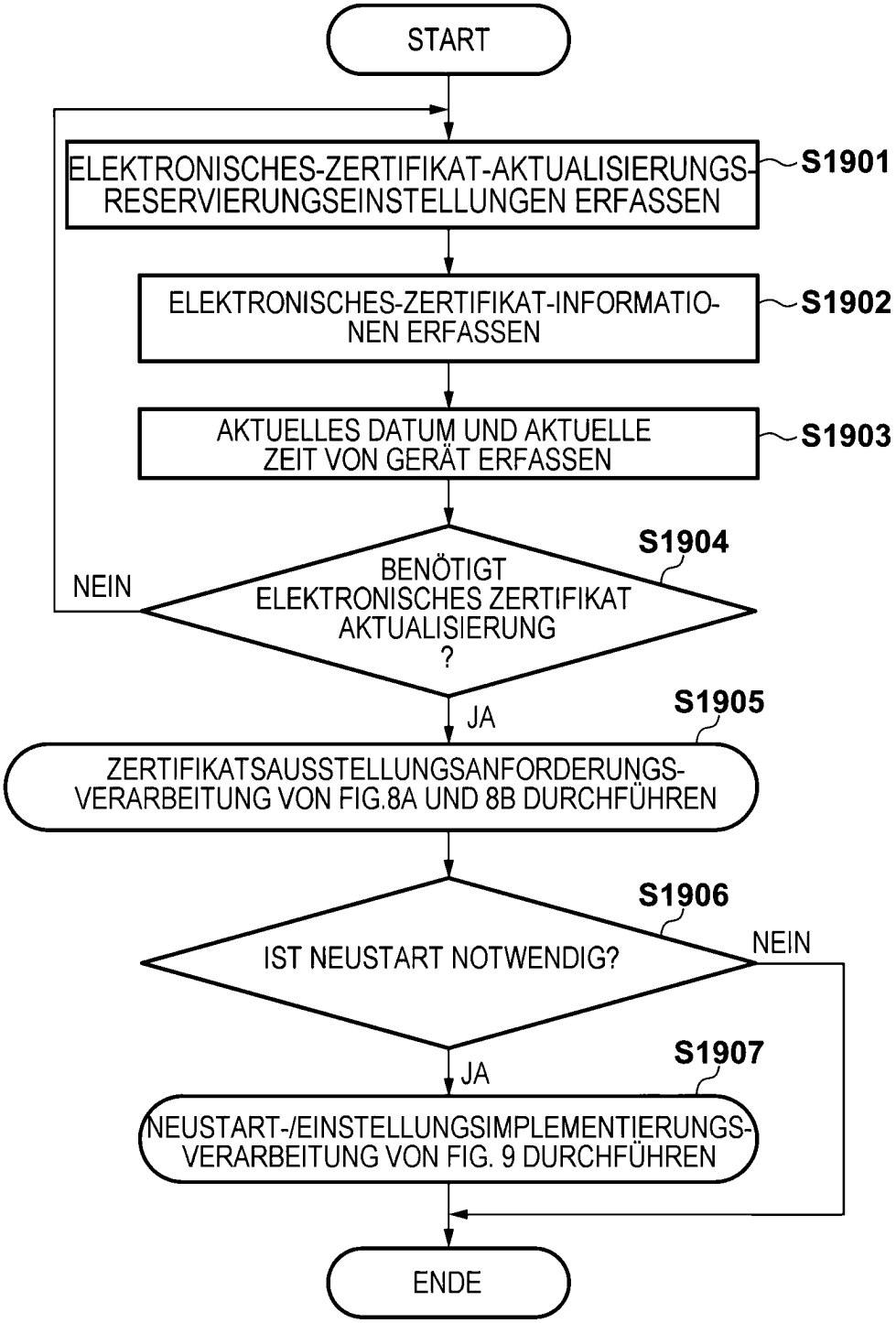

ZERTIFIKATSERFASSUNGSANFORDERUNG/EINSTELLUNGSBILDSCHIRM
ZERTIFIKATSLISTE
VERBINDUNGS-EINSTELLUNGEN
CA-ZERTIFIKAT-ERFASSUNG
ZERTIFKATS-AUSSTELLUNGS-ANFORDERUNG
RESERVIERUNGS-EINSTELLUNG
ELEKTRONISCHES-ZERTIFIKAT-AKTUALISIERUNGSRESERVIERUNGSEINSTELLUNG
1801
BEZEICHNEN EINES AKTUALISIERUNGSDATUMS
ERFASSUNGSANFORDERUNG-STARTDATUM
JAHR
MONAT
TAG
ERFASSUNGSANFORDERUNG-STARTZEIT
STUNDE
MINUTE
1802
AKTUALISIERUNG DES ELEKTRONISCHEN ZERTIFIKATS, FALLS EINE ANZAHL VON TAGEN VOR DEM ABLAUF DER GÜLTIG-KEITSDAUER DES AKTUELL VERWENDETEN ELEKTRONISCHEN ZERTIFIKATS EINE VORBESTIMMTE ANZAHL ODER WENIGER IST
14
TAGE VOR DEM ABLAUF DER GÜLTIGKEITSDAUER
1803
AKTUALISIERUNG BASIEREND AUF VORBESTIMMTEM ZYKLUS
AKTUALISIERUNG IM
TAGE-INTERVALL
AKTUALISIERUNG AM
TAG VOR JEDEM MONAT
AKTUALISIERUNG AM
MONAT
TAG VON JEDEM JAHR

FIG. 19


START
ELEKTRONISCHES-ZERTIFIKAT-AKTUALISIERUNGS-RESERVIERUNGSEINSTELLUNGEN ERFASSEN
S1901
ELEKTRONISCHES-ZERTIFIKAT-INFORMATIONEN ERFASSEN
S1902
AKTUELLES DATUM UND AKTUELLE ZEIT VON GERÄT ERFASSEN
S1903
BENÖTIGT ELEKTRONISCHES ZERTIFIKAT AKTUALISIERUNG ?
S1904
NEIN
JA
ZERTIFIKATSAUSSTELLUNGSANFORDERUNGS-VERARBEITUNG VON FIG.8A UND 8B DURCHFÜHREN
S1905
IST NEUSTART NOTWENDIG?
S1906
NEIN
JA
NEUSTART-/EINSTELLUNGSIMPLEMENTIERUNGS-VERARBEITUNG VON FIG. 9 DURCHFÜHREN
S1907
ENDE