(19) Deutsches Patent- und Markenamt

(10) **DE 10 2014 210 058 A1** 2014.12.04

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2014 210 058.5**
(22) Anmeldetag: **27.05.2014**
(43) Offenlegungstag: **04.12.2014**

(51) Int Cl.: ***H04L 9/32*** (2006.01)

(30) Unionspriorität:
2013-111839 28.05.2013 JP

(71) Anmelder:
CANON KABUSHIKI KAISHA, Tokio, JP

(74) Vertreter:
TBK, 80336 München, DE

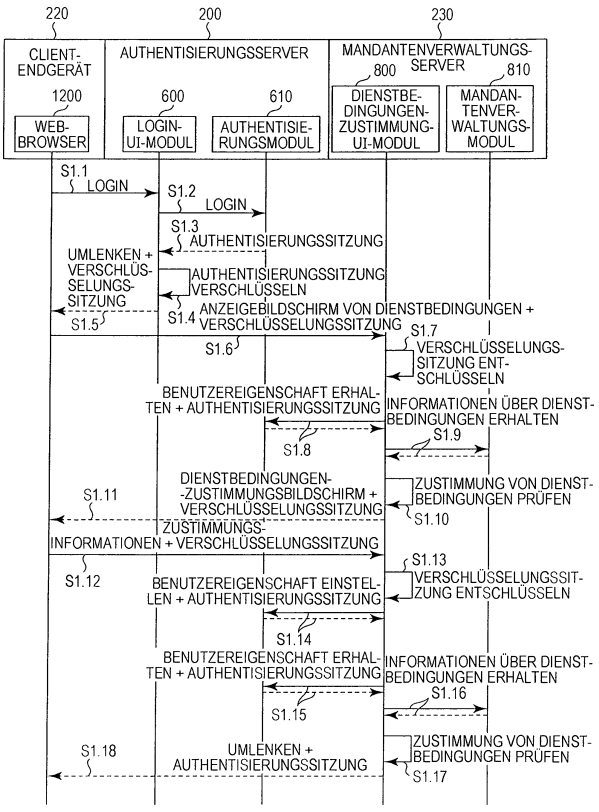
(72) Erfinder:
Mihara, Makoto, c/o CANON KABUSHIKI KAISHA, Tokio, JP

Prüfungsantrag gemäß § 44 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Informationsverarbeitungsserversystem, Steuerverfahren und Programm**

(57) Zusammenfassung: Es ist ein Informationsverarbeitungsserversystem bereitgestellt, in dem eine Zustimmung zu Dienstbedingungen durch einen Benutzer unter Verwendung einer zweiten Authentisierungssitzung bestätigt wird, die sich von einer ersten Authentisierungssitzung unterscheidet, die verwendet wird, wenn ein Client den Webdienst verwendet.



Beschreibung

HINTERGRUND

Gebiet

[0001] Aspekte der vorliegenden Erfindung beziehen sich im Allgemeinen auf ein Informationsverarbeitungsserversystem, das eine Verwendung von einem Webdienst gemäß einer Zustimmung zu Bedingungen des Webdiensts startet, ein Steuerverfahren und ein Programm.

Beschreibung der verwandten Technik

[0002] In den letzten Jahren wurde weithin ein Geschäftsmodell angeboten, in dem Dienste für Kunden unter Verwendung von im Internet bereitgestellten Servern, wie etwa Cloud-Dienste, bereitgestellt werden. In einem solchen Geschäftsmodell werden unterschiedliche Dienste bereitgestellt, und wählt ein Kunde einen gewünschten der Dienste aus und schließt er einen Vertrag nur für den erforderlichen Dienst ab.

[0003] Wenn ein derartiger Dienst für eine bestimmte Kundenfirma bereitgestellt wird, erzeugt außerdem ein Dienstanbieter einen Mandanten neu, der der Kundenfirma zuzuordnen ist. Außerdem wird ein Erstbenutzer, der den neu erzeugten Mandanten auf der Seite der Kundenfirma verwaltet, erzeugt und in dem Mandanten registriert. Ein Administrator der Kundenfirma loggt bzw. wählt sich als der erzeugte Erstbenutzer in den Dienst ein und fügt den Benutzer zu dem zugeordneten Mandanten hinzu, und zusätzlich führt er erforderliche Einstellungen durch, so dass die Kundenfirma eine Verwendung des Diensts starten kann.

[0004] Der Benutzer, der den Dienst tatsächlich verwendet, wird aufgefordert, durch den Dienstanbieter definierten Dienstbedingungen und einer Verwendung von persönlichen Informationen zuzustimmen, wenn er sich zum ersten Mal in den Dienst einloggt bzw. -wählt. Erst nach einer Zustimmung zu den Dienstbedingungen und der Verwendung von persönlichen Informationen kann der Benutzer in einigen Fällen sich einloggen bzw. -wählen und den Dienst verwenden. Was die Dienstbedingungen betrifft, kann der Benutzer aufgefordert werden, unterschiedlichen Dienstbedingungen für unterschiedliche Dienste zuzustimmen, oder aufgefordert werden, den gleichen Dienstbedingungen zuzustimmen, die von unterschiedlichen Diensten gemeinsam genutzt werden, um so alle diese Dienste zu verwenden.

[0005] Im Allgemeinen wird ein Zugriff auf einen durch eine Authentisierungsfunktion geschützten Server unter Verwendung von einem Cookie durchgeführt, nachdem eine Authentisierungssitzung, die darstellt, dass eine Authentisierung erfolgreich durchgeführt ist, als Ergebnis von einem Einloggen bzw. -wählen in den Dienst in einem Webbrowser von einem Client als das Cookie gespeichert ist. Wenn auf durch den Server bereitgestellte Webseiten zuzugreifen ist, überträgt der Client ein Cookie an den Server. Dann bestimmt der Server, dass die Zugriffe auf die Webseiten durch den gleichen Benutzer durchgeführt werden, und stellt er den Dienst an den Benutzer bereit. Wenn ein Cookie einer Authentisierungssitzung an einen Webbrowser von einem Client geliefert ist, darf der Webbrowser auf eine durch eine Authentisierungsfunktion geschützte Webseite zugreifen, wie es in dem japanischen Patent Nr. 4056390 offenbart ist.

[0006] Wenn eine Zustimmung zu Dienstbedingungen und einer Verwendung von persönlichen Informationen von jedem Benutzer gefordert wird, führt der Benutzer ein Login unter Verwendung von einem Login-Bildschirm eines Servers durch. Der Server erhält Informationen über einen durch den Benutzer verwendbaren Dienst und Informationen über Dienstbedingungen, denen der Benutzer zugestimmt hat, und stellt einen Bildschirm zum Vornehmen einer Zustimmung zu Dienstbedingungen bereit, für die bestimmt wird, dass der Benutzer nicht zugestimmt hat. Wenn ein Ergebnis einer Zustimmung durch den Benutzer über den Zustimmungsbildschirm an den Server geliefert wird, erfordert der Server ein Cookie einer Authentisierungssitzung, um so den Benutzer zu spezifizieren, der den Dienstbedingungen zugestimmt hat.

[0007] Wenn das Cookie der Authentisierungssitzung an einen Webbrowser geliefert wird, ist jedoch es möglich, dass ein Webdienst ohne die Zustimmung zu den Dienstbedingungen verfügbar wird. Im Speziellen kann der Benutzer, wenn der Benutzer eine URL des Diensts unter Verwendung des Webbrowsers direkt angibt, während der Zustimmungsbildschirm angezeigt wird, ohne die Zustimmung zu den Dienstbedingungen auf den Webdienst zugreifen und diesen Verwenden.

KURZFASSUNG DER ERFINDUNG

[0008] Aspekte der vorliegenden Erfindung stellen im Allgemeinen ein Informationsverarbeitungsserversystem bereit, in dem eine Zustimmung zu Dienstbedingungen durch einen Benutzer unter Verwendung einer Authentisierungssitzung bestätigt wird, die sich von einer Authentisierungssitzung unterscheidet, die verwendet wird, wenn ein Client einen Webdienst verwendet.

[0009] Gemäß einem Aspekt der vorliegenden Erfindung umfasst ein Informationsverarbeitungsserversystem eine Erzeugungseinheit, die konfiguriert ist zum Erzeugen einer zweiten Authentisierungssitzung basierend auf einer ersten Authentisierungssitzung,

die erzeugt wird, nachdem ein Benutzer authentisiert ist, und die verwendet wird, wenn ein Client einen Webdienst verwendet, eine Übertragungseinheit, die konfiguriert ist zum Übertragen der zweiten Authentisierungssitzung an den Client, und eine Empfangseinheit, die konfiguriert ist zum Empfangen der zweiten Authentisierungssitzung zusammen mit Informationen, die eine Zustimmung zu Bedingungen des Webdiensts darstellen, von dem Client. Die Übertragungseinheit überträgt die erste Authentisierungssitzung, die der zweiten Authentisierungssitzung entspricht, an den Client, wenn gemäß den empfangenen Informationen und der zweiten Authentisierungssitzung bestimmt wird, dass der Benutzer den Bedingungen des Webdiensts zugestimmt hat.

[0010] Weitere Merkmale der vorliegenden Offenbarung werden aus der folgenden Beschreibung von beispielhaften Ausführungsbeispielen unter Bezugnahme auf die begleitenden Zeichnungen ersichtlich.

KURZE BESCHREIBUNG DER ZEICHNUNGEN

[0011] **Fig.** 1 ist eine Darstellung, die eine Systemkonfiguration veranschaulicht.

[0012] **Fig.** 2 ist eine Darstellung, die eine Hardwarekonfiguration von Vorrichtungen veranschaulicht.

[0013] **Fig.** 3 ist eine Darstellung, die Konfigurationen von Softwaremodulen veranschaulicht.

[0014] **Fig.** 4 ist eine Darstellung, die eine Konfiguration von einer durch einen Authentisierungsserver verwalteten Tabelle veranschaulicht.

[0015] **Fig.** 5A und **Fig.** 5B sind Darstellungen, die Konfigurationen von durch einen Mandantenverwaltungsserver verwalteten Tabellen darstellen.

[0016] **Fig.** 6 ist eine Darstellung, die einen Ablauf von Login und Zustimmung zu Dienstbedingungen veranschaulicht.

[0017] **Fig.** 7 ist ein Ablaufdiagramm, das einen Prozess zum Bestimmen veranschaulicht, ob eine Zustimmung zu den Dienstbedingungen erforderlich ist.

[0018] **Fig.** 8A und **Fig.** 8B sind Darstellungen, die Bildschirme mit Bezug auf die Dienstbedingungen veranschaulichen.

[0019] **Fig.** 9 ist eine Darstellung, die einen Ablauf von Einmal- bzw. Einzelanmeldung und Anzeige von einem Dienstbedingungen-Zustimmungsbildschirm veranschaulicht.

[0020] **Fig.** 10 ist ein Ablaufdiagramm, das einen Prozess zum Bestimmen von einer SAML-Verifikationserfolgsantwort veranschaulicht.

[0021] **Fig.** 11 ist eine Darstellung, die eine Konfiguration von einer durch einen Authentisierungsserver verwalteten Temporärsitzungsverwaltungstabelle veranschaulicht.

BESCHREIBUNG DER AUSFÜHRUNGSBEISPIELE

[0022] Nachstehend werden hierin beispielhafte Ausführungsbeispiele unter Bezugnahme auf die begleitenden Zeichnungen beschrieben.

[0023] Bei diesen Ausführungsbeispielen wird angenommen, dass ein Formulardienst zum Erzeugen eines Formulars im Internet und ein Druckdienst zum Drucken des erzeugten Formulars unter Verwendung einer Bilderzeugungsvorrichtung durch einen Server im Internet bereitgestellt werden. Nachstehend werden hierin Dienste einschließlich der vorstehend beschriebenen Dienste, die ihre Funktionen im Internet bereitstellen, als ”Webdienste” bezeichnet.

Erstes Ausführungsbeispiel

[0024] Ein Dienstbedingungen-Verwaltungssystem gemäß einem ersten Ausführungsbeispiel wird in einem Netzwerk verwirklicht, das konfiguriert ist, wie es in **Fig.** 1 veranschaulicht ist. Ein WWW-System (WWW: ”World Wide Web”) ist als ein Weitverkehrsnetzwerk (WAN: ”Wide Area Network”) **100** gemäß der vorliegenden Technik aufgebaut. Lokale Netzwerke (LAN: ”Local Area Network”) **101** verbinden Komponenten miteinander.

[0025] Ein Authentisierungsserver **200** authentisiert Benutzer. Ein Ressourcenserver **210** stellt Webdienste einschließlich eines Formulardiensts und eines Druckdiensts bereit. Ein einzelner Ressourcenserver kann einen einzelnen Webdienst oder eine Vielzahl von Webdiensten umfassen. Außerdem kann, obwohl ein einzelner Server als jeder der Server bereitgestellt ist, eine Vielzahl von Server als jeder der Server bereitgestellt sein. Daher spezifiziert der Begriff ”Informationsverarbeitungsserversystem” zumindest einen Server. Ein Clientendgerät **220** umfasst einen darauf installierten Webbrowser. Ein Mandantenverwaltungsserver **230** führt eine Verwaltung von Inhalt der Dienstbedingungen und einer Erzeugung von einem Zustimmungsbildschirm durch. Ein Identitätslieferant (IdP: ”Identity Provider”) **240** von einer ”Security Assertion Markup Language” (SAML) für eine Einmal- bzw. Einzelanmeldung ist ein Authentisierungsserver, der separat von diesem System bereitgestellt ist. Außerdem sind der Authentisierungsserver **200**, der Ressourcenserver **210**, das Clientendgerät **220**, der Mandantenverwaltungsserver **230** und der IdP **240** über das WAN **100** und die LANs **101** miteinander verbunden. Hier können der Authentisierungsserver **200**, der Ressourcenserver **210**, das Clientendgerät **220**, der Mandantenverwaltungsser-

ver **230** und der IdP **240** in jeweiligen LANs konfiguriert sein oder in dem gleichen LAN konfiguriert sein. Außerdem können der Authentisierungsserver **200**, der Ressourcenserver **210** und der Mandantenserverwaltungsserver **230** in dem gleichen Server konfiguriert sein.

[0026] Es ist zu beachten, dass das vorstehend beschriebene Informationsverarbeitungsserversystem zumindest einen Login-Steuerserver, der einen Benutzerauthentisierungsprozess durchführt, und einen Ressourcenserver, der einen Dienst bereitstellt, wenn der Benutzerauthentisierungsprozess durch den Login-Steuerserver erfolgreich durchgeführt wird, umfasst. Es wird jedoch auch eine Konfiguration angenommen, in der die Server als ein einzelner Server integriert sind, und daher ist es, wenn der Begriff "Informationsverarbeitungsserversystem" verwendet wird, nicht notwendiger Weise der Fall, dass das Informationsverarbeitungsserversystem, das eine Vielzahl von Diensten bereitstellt, eine Vielzahl von Server umfasst. Außerdem kann das Informationsverarbeitungsserversystem nur den Login-Steuerserver oder nur den Ressourcenserver umfassen.

[0027] **Fig.** 2 ist eine Darstellung, die eine Konfiguration des Clientendgeräts **220** gemäß diesem Ausführungsbeispiel veranschaulicht. Die Servercomputer, die den Authentisierungsserver **200**, den Ressourcenserver **210**, den Mandantenverwaltungsserver **230** und den IdP **240** umfassen, weisen die gleichen Konfigurationen auf. Hier entspricht eine Darstellung von Hardwareblöcken, die in **Fig.** 2 veranschaulicht ist, einer Darstellung von Hardwareblöcken von allgemeinen Informationsverarbeitungsvorrichtungen, und kann eine Hardwarekonfiguration der allgemeinen Informationsverarbeitungsvorrichtungen auf das Clientendgerät **220** und die Servercomputer gemäß diesem Ausführungsbeispiel angewandt werden.

[0028] Gemäß **Fig.** 2 führt eine CPU **231** ein OS und Anwendungen umfassende Programme aus, die in einem ROM **233** zum Speichern von Programmen gespeichert sind oder von einem externen Speicher **241** wie etwa einer Festplatte (HD) in einen RAM **232** geladen werden. Außerdem steuert die CPU **231** die mit einem Systembus **234** verbundenen Blöcke. Hier ist der Begriff "OS" eine Abkürzung für ein auf einem Computer laufendes Betriebssystem, und ein Betriebssystem wird hierin nachstehend als "OS" bezeichnet. Prozesse von Abläufen, die hierin nachstehend beschrieben werden, werden verwirklicht, wenn Programme ausgeführt werden. Der RAM **232** fungiert als ein Hauptspeicher, ein Arbeitsbereich und dergleichen von der CPU **231**. Eine Tastatursteuereinheit (KBC: "Keyboard Controller") **235** steuert eine durch eine Tastatur **239** und eine nicht veranschaulichte Zeigevorrichtung durchgeführte Tasteneingabe. Eine CRT-Steuereinheit (CRTC: "CRT Controller") **236** steuert eine Anzeige von einer CRT-Anzeige **242**. Eine Plattensteuereinheit (DKC: "Disk Controller") **237** steuert einen Datenzugriff in dem externen Speicher **241** wie etwa einer verschiedene Daten speichernden Festplatte (HD). Eine Netzwerksteuereinheit (NC: "Network Controller") **238** führt einen Prozess der Steuerung einer Kommunikation mit den Servercomputern und anderen Vorrichtung durch, die über das WAN **100** oder die LANs **101** verbunden sind. In der nachstehenden Beschreibung ist die CPU **231** ein Hauptteil von Hardware für eine durch den Server durchgeführte Ausführung, sofern es nicht anderweitig angegeben ist, und sind Anwendungsprogramme, die in dem externen Speicher **241** installiert sind, ein Hauptteil von Software.

[0029] **Fig.** 3 ist eine Darstellung, die Konfigurationen von Modulen von dem Authentisierungsserver **200**, dem Ressourcenserver **210**, dem Clientendgerät **220**, dem Mandantenverwaltungsserver **230** und dem IdP **240** veranschaulicht. Der Authentisierungsserver **200** umfasst ein Login-UI-Modul **600**, ein Authentisierungsmodul **610** und ein SSO-Hook-Modul **620**. Der Ressourcenserver **210** umfasst ein Ressourcenservermodul **700**. Das Clientendgerät **220** umfasst einen Webbrowser **1000**, der ein Benutzeragent zur Verwendung von dem WWW ist. Der Mandantenverwaltungsserver **230** umfasst ein Dienstbedingungen-Zustimmung-UI-Modul **800** und ein Mandantenverwaltungsmodul **810**. Der IdP **240** umfasst ein Login-UI-Modul **900** und ein Authentisierungsmodul **910**.

[0030] **Fig.** 4 ist eine Darstellung, die eine Datentabelle veranschaulicht, die in einem externen Speicher durch den Authentisierungsserver **200** gespeichert wird. Anstelle des externen Speichers des Authentisierungsservers **200** kann die Datentabelle in einem anderen Server gespeichert werden, mit dem über das LAN **101** kommuniziert werden kann. Eine Benutzerverwaltungstabelle **1200** umfasst eine Benutzer-ID **1201**, ein Passwort **1202**, eine Mandant-ID **1203**, eine Rolle **1204**, Dienstbedingungen-Zustimmungsinformationen **1205** und Sitzungsinformationen **1206**. Der Authentisierungsserver **200** hat eine Funktion zum Verifizieren einer Kombination von Informationen über die Benutzer-ID **1201** und Informationen über das Passwort **1202**, Authentisieren von jedem Benutzer und Erzeugen von einer Authentisierungssitzung. Das Clientendgerät **220** darf auf einen Webdienst durch Verwendung der Authentisierungssitzung zugreifen. Die Rolle **1204** stellt Informationen über eine Berechtigung von jedem Benutzer dar. Hier stellt "KUNDENADMIN" eine Berechtigung eines Administrators dar, stellt "KUNDE" eine Berechtigung eines allgemeinen Benutzers dar, stellt "FORMULAR" eine Berechtigung zur Verwendung des Formulardiensts dar, und stellt "DRUCK" eine Berechtigung zur Verwendung des Druckdiensts dar. Nur die Rollen, die in "FORMULAR" und "DRUCK" entsprechen,

ermöglichen eine Verwendung der entsprechenden Webdienste. Die Dienstbedingungen-Zustimmungsinformationen **1205** stellen Dienstbedingungen dar, denen jeder Benutzer zugestimmt hat. Die Sitzungsinformationen **1206** stellen einen Bereich dar, der erzeugte Authentisierungssitzungen speichert. IDs von Authentisierungssitzungen, die durch das System eindeutig bestimmt werden, und Ablauf- bzw. Verfallsdaten der Authentisierungssitzungen sind in den Sitzungsinformationen **1206** gespeichert.

[0031] **Fig.** 5A und **Fig.** 5B sind Darstellungen, die Datentabellen veranschaulichen, die in einem externen Speicher durch den Mandantenverwaltungsserver **230** gespeichert werden. Anstelle des externen Speichers des Mandantenverwaltungsservers **230** können die Datentabellen in einem anderen Server gespeichert werden, mit dem über das LAN **101** kommuniziert werden kann. In **Fig.** 5A ist eine Lizenzverwaltungstabelle **1500** veranschaulicht. Die Lizenzverwaltungstabelle **1500** umfasst eine Mandant-ID **1501**, eine Verkaufsmandant-ID **1502**, eine Lizenz **1503** und eine Lizenzzählung bzw. -zahl **1504**. Die Lizenzverwaltungstabelle **1500** verwaltet für Kundenmandanten verfügbare Webdienste. Bei dem ersten Ausführungsbeispiel stellen Informationen dar, dass ein Kundenmandant, der einer Mandant-ID **1501** ”1001 AA” entspricht, Lizenzen **1503** ”FORMULAR” und ”DRUCK” verwenden kann, die einer Lizenzzählung **1504** ”20” entsprechen, wobei diese durch einen Verkaufsmandanten bereitgestellt sind, der einer Verkaufsmandant-ID **1502** ”101AA” entspricht.

[0032] In **Fig.** 5B ist eine Dienstbedingungenverwaltungstabelle **1600** veranschaulicht. Die Dienstbedingungenverwaltungstabelle **1600** umfasst eine Dienstbedingungen-ID **1601**, eine Verkaufsmandant-ID **1602**, eine Lizenz **1603**, eine Änderung **1604** und Inhalt **1605**. Die Dienstbedingungenverwaltungstabelle **1600** verwaltet Dienstbedingungen, die Lizenzen für einzelne Verkaufsmandanten entsprechen, die die Lizenzen verkaufen. Die Dienstbedingungen-ID **1601** wird verwendet, um Dienstbedingungen in dem System eindeutig zu identifizieren. Die Verkaufsmandant-ID **1602** verwaltet Mandanten, die Lizenzen verkauft haben. Die Lizenz **1603** verwaltet Lizenzen, die den anzuzeigenden Dienstbedingungen entsprechen. Bei diesem Ausführungsbeispiel sind verschiedene Typen von Dienstbedingungen definiert, einschließlich Dienstbedingungen für eine ”FORMULAR”-Lizenz, Dienstbedingungen für eine ”DRUCK”-Lizenz und Dienstbedingungen, die von der ”FORMULAR”-Lizenz und der ”DRUCK”-Lizenz geteilt bzw. gemeinsam genutzt werden, und verwaltet die Änderung **1604** Änderungen der verschiedenen Typen von Dienstbedingungen. Informationen über die Änderung **1604** werden gespeichert, da, wenn Dienstbedingungen geändert werden, denen der Benutzer zugestimmt hat, ein Prozess zum Anfordern einer Zustimmung zu den Dienstbedingungen, die geändert wurden, erneut verwirklicht wird. Der Inhalt **1605** verwaltet einen Inhalt von Dienstbedingungen, für die es in der Praxis erforderlich ist, dass der Benutzer zustimmt.

[0033] Unter Bezugnahme auf **Fig.** 6 wird ein Ablauf von Prozessen gemäß diesem Ausführungsbeispiel beschrieben, in denen der Benutzer ein Login von einer Webseite durchführt und Dienstbedingungen zustimmt, sowie eine Verwendung von einem Webdienst gestartet wird. Dieser Ablauf wird durchgeführt, wenn sich der Benutzer unter Verwendung von dem Webbrowser **1000** des Clientendgeräts **220** in das Informationsverarbeitungsserversystem einloggt.

[0034] Zunächst greift der Webbrowser **1000** auf das Login-UI-Modul **600** des Authentisierungsservers **200** zu, um ein Login durchzuführen (S1.1). In diesem Prozess gibt der Systembenutzer Benutzerauthentisierungsinformationen einschließlich einer Benutzer-ID und eines Passworts ein. Das Login-UI-Modul **600** überträgt die Benutzer-ID und das Passwort an das Authentisierungsmodul **610** (S1.2). Nach Prüfung einer Übereinstimmung von der empfangenen Benutzer-ID und dem empfangenen Passwort mit Bezug auf Daten, die in der Benutzerverwaltungstabelle **1200** umfasst sind, und Bestimmung, dass eine Authentisierung erfolgreich durchgeführt ist, erzeugt das Authentisierungsmodul **610** eine Authentisierungssitzung bzw. Authentisierungssitzungsinformationen. Das Authentisierungsmodul **610** speichert die erzeugte Authentisierungssitzung bzw. die erzeugten Authentisierungssitzungsinformationen in den Sitzungsinformationen **1206** der Benutzerverwaltungstabelle **1200** und überträgt daraufhin eine Antwort an das Login-UI-Modul **600** (S1.3). Das Login-UI-Modul **600** verschlüsselt die in Schritt S1.3 erhaltene Authentisierungssitzung (S1.4). Ein für die Verschlüsselung verwendeter Verschlüsselungsschlüssel wird nur von dem Login-UI-Modul **600** und dem Dienstbedingungen-Zustimmung-UI-Modul **800** geteilt bzw. gemeinsam genutzt. Daher können die Verschlüsselung und die Entschlüsselung der Authentisierungssitzung nur durch das Login-UI-Modul **600** und das Dienstbedingungen-Zustimmung-UI-Modul **800** durchgeführt werden. Das Login-UI-Modul **600** stellt eine Verschlüsselungssitzung auf ein Cookie ein und überträgt eine Antwort, die eine Umlenkung bzw. -schaltung auf einen Dienstbedingungen-Zustimmungsbildschirm darstellt, an das Clientendgerät **220** (S1-5).

[0035] Bei Empfang einer Anweisung zur Umlenkung bzw. -schaltung überträgt der Webbrowser **1000** eine Anforderung zum Erhalten des Dienstbedingungen-Zustimmungsbildschirms an das Dienstbedingungen-Zustimmung-UI-Modul **800** des Mandantenverwaltungsservers **230**. Gleichzeitig überträgt der Webbrowser **1000** auch Informationen über

die Verschlüsselungssitzung (S1.6). Das Dienstbedingungen-Zustimmung-UI-Modul **800** erhält die Verschlüsselungssitzung aus der von dem Webbrowser **1000** gelieferten Anforderung und führt einen Verschlüsselungsprozess durch, um Informationen über die Authentisierungssitzung zu erhalten (S1.7). Das Dienstbedingungen-Zustimmung-UI-Modul **800** überträgt die erhaltenen Informationen über die Authentisierungssitzung an das Authentisierungsmodul **610** und erhält eine Benutzereigenschaft (S1.8). Das Authentisierungsmodul **610** spezifiziert einen Benutzer, der der Authentisierungssitzung entspricht, aus den Sitzungsinformationen **1206** der Benutzerverwaltungstabelle **1200** und erhält Daten einschließlich der Benutzer-ID **1201**, des Passworts **1202**, der Mandant-ID **1203**, der Rolle **1204** und der Dienstbedingungen-Zustimmungsinformationen **1205**. Das Authentisierungsmodul **610** überträgt die erhaltenen Informationen an das Dienstbedingungen-Zustimmung-UI-Modul **800** als Antwort (S1.8). Das Dienstbedingungen-Zustimmung-UI-Modul **800** fragt an dem Mandantenverwaltungsmodul **810** bezüglich Informationen über die in Schritt S1.8 erhaltene Mandant-ID **1203** an und erhält Informationen über Dienstbedingungen (S1.9). Das Mandantenverwaltungsmodul **810** erhält Informationen über Dienstbedingungen, für die eine Zustimmung erforderlich ist, in einem Zielmandanten mit Bezug auf die Lizenzverwaltungstabelle **1500** und die Dienstbedingungenverwaltungstabelle **1600**. Zum Beispiel, wenn eine Mandant-ID ”1001AA” geliefert wird, werden Informationen über Dienstbedingungen erhalten, die einer Dienstbedingungen-ID **1601** ”2” (Dienstbedingungen einer neuesten Änderung der ”FORMULAR”-Lizenz, die durch den Mandanten mit der Verkaufsmandant-ID **1502** ”101AA” verkauft ist) und einer Dienstbedingungen-ID **1601** ”3” (Dienstbedingungen einer neuesten Änderung der ”DRUCK”-Lizenz, die durch den Mandanten mit der Verkaufsmandant-ID **1502** ”101 AA” verkauft ist) entsprechen. Das Mandantenverwaltungsmodul **810** überträgt die erhaltenen Informationen über die Dienstbedingungen an das Dienstbedingungen-Zustimmung-UI-Modul **800** als Antwort (S1.9). Das Dienstbedingungen-Zustimmung-UI-Modul **800** prüft, ob Dienstbedingungen existieren, für die es erforderlich ist, dass eine Zustimmung vorgenommen wird, unter Verwendung der in Schritt S1.8 erhaltenen Benutzereigenschaft und den in Schritt S1.9 erhaltenen Informationen über die Dienstbedingungen (S1.10).

[0036] Unter Bezugnahme auf **Fig.** 7 wird hier ein Ablauf von einem Prozess zum Bestimmen, ob Dienstbedingungen existieren, für die es erforderlich ist, dass eine Zustimmung vorgenommen wird, in Schritt S1.10 ausführlich beschrieben. In diesem Prozess werden unterschiedlich Verfahren der Bestimmung dahingehend, ob Dienstbedingungen existieren, für die es erforderlich ist, dass eine Zustimmung vorgenommen wird, zwischen dem Administrator und einem allgemeinen Benutzer eingesetzt. Der allgemeine Benutzer nimmt die Bestimmung gemäß einer geeigneten Rolle vor, die dem Benutzer zuordnet ist, um einen Webdienst zu verwenden, der einer dem Benutzer zugeordneten Lizenz entspricht. Der Administrator kann in einigen Fällen keine Rolle eines speziellen Webdiensts wie etwa Benutzerverwaltung und Mandantenverwaltung haben. Dies ist deshalb so, da der Administrator in der Praxis einem Konto zum Verwalten von Benutzern des gleichen Mandanten, die Webdienste verwenden, anstelle von einem Konto zur Verwendung von Webdiensten entspricht. Selbst wenn der Administrator keine einer Lizenz entsprechende Rolle hat, ist es daher erforderlich, dass der Administrator Dienstbedingungen zustimmt, um sich in das System einzuloggen. Dementsprechend nimmt der Administrator die Bestimmung dahingehend, ob Dienstbedingungen existieren, für die es erforderlich ist, dass eine Zustimmung vorgenommen wird, gemäß einer Bestimmung dahingehend vor, ob eine Lizenz existiert, die durch einen Mandanten verkauft ist, zu dem der Administrator gehört.

[0037] In Schritt S1.10 wird gemäß der Benutzereigenschaft bestimmt, ob der Benutzer der Administrator oder der allgemeine Benutzer ist (52.1). Wenn der Benutzer ein allgemeiner Benutzer ist, schreitet der Prozess zu Schritt S2.2 voran und wird die Bestimmung dahingehend, ob Dienstbedingungen existieren, für die es erforderlich ist, dass eine Zustimmung vorgenommen wird, gemäß einer dem Benutzer zugeordneten Rolle vorgenommen. Nachstehend wird hierin eine Beschreibung auf Grundlage von Informationen über Benutzer vorgenommen, die durch die Benutzerverwaltungstabelle **1200** definiert sind. In Schritt S2.2 wird bestimmt, ob eine einer Lizenz entsprechende Rolle dem Benutzer zugeordnet wurde. Wenn die Rolle nicht zugeordnet wurde, schreitet der Prozess zu Schritt S2.5 voran, in dem sich der Benutzer nicht einloggen darf und eine Verwendung des Systems verboten bzw. gesperrt/gestoppt wird. In einem Fall von ”Benutzer2” ist die Rolle ”DRUCK” zugeordnet und schreitet der Prozess daher zu Schritt S2.3 voran. In Schritt S2.3 wird ein Schleifenprozess mit einer Häufigkeit durchgeführt, die der Anzahl von dem Benutzer zugeordneten Rollen entspricht. In dem Fall von ”Benutzer2” wird der Schleifenprozess einmal für die Rolle ”DRUCK” durchgeführt, und in einem Fall von ”Benutzer3” wird der Schleifenprozess zweimal für die Rollen ”FORMULAR” und ”DRUCK” durchgeführt. In Schritt S2.4 wird bestimmt, ob der Benutzer entsprechenden Dienstbedingungen zugestimmt hat. In dem Fall von ”Benutzer2”, da der ”Benutzer2” zu der Mandant-ID ”1001 AA” gehört, wird eine Lizenz ”DRUCK”, was ein Webdienst ist, der mit einem der Verkaufsmandant-ID ”101AA” entsprechenden Mandanten in Zusammenhang steht und an den Zielmandanten verkauft ist, gemäß in der Lizenzverwaltungstabelle **1500** umfassten Informationen spezifiziert. Außerdem werden

gemäß in der Dienstbedingungenverwaltungstabelle **1600** umfassten Informationen Dienstbedingungen spezifiziert, die der Dienstbedingungen-ID **1601** ”3” entspricht. Da keine Informationen über eine Zustimmung zu den Dienstbedingungen in den Dienstbedingungen-Zustimmungsinformationen **1205** aufgezeichnet wurden, die ”Benutzer2” entsprechen, wird in Schritt S2.7 ein Prozess durchgeführt, der durchzuführen ist, wenn Dienstbedingungen existieren, für die es erforderlich ist, dass eine Zustimmung vorgenommen wird. Wie bei dem Fall von ”Benutzer1” wird, wenn der Benutzer entsprechenden Dienstbedingungen zugestimmt hat, in Schritt S2.6 ein Prozess durchgeführt, der durchzuführen ist, wenn Dienstbedingungen nicht existieren, für die es erforderlich ist, dass eine Zustimmung vorgenommen wird. Durch diesen Prozess wird ein Prozess zum Bestimmen abgeschlossen, ob eine Prozess zur Zustimmung zu Dienstbedingungen erforderlich ist, wenn der Benutzer ein allgemeiner Benutzer ist.

[0038] Die Beschreibung kehrt zu Schritt S2.1 zurück. Wenn der Benutzer ein Administrator ist, schreitet der Prozess zu Schritt S2.10 voran, in dem Dienstbedingungen gemäß einer Lizenz bestimmt werden, die an einen Mandanten verkauft ist, zu dem der Benutzer gehört. In Schritt S2.10 wird ein Schleifenprozess mit einer Häufigkeit durchgeführt, die Lizenzen entspricht, die dem Mandanten zugeordnet sind, zu dem der Benutzer gehört. In einem Fall von ”Admin1” wird, da ”Admin1” zu einem Mandanten mit der Mandant-ID ”1001AA” gehört, der Schleifenprozess gemäß den in der Lizenzverwaltungstabelle **1500** umfassten Informationen zweimal durchgeführt, nämlich mit einer Häufigkeit, die der Anzahl von Lizenzen entspricht, nämlich der ”FORMULAR”-Lizenz und der ”DRUCK”-Lizenz. Durch diesen Prozess kann selbst der Administrator, dem keine Rolle zugeordnet ist, geeignete Dienstbedingungen erhalten. In Schritt S2.11 wird bestimmt, ob der Benutzer entsprechenden Dienstbedingungen zugestimmt hat. In dem Fall von ”Admin1” wird gemäß den in der Lizenzverwaltungstabelle **1500** umfassten Informationen die Verkaufsmandant-ID ”101AA” spezifiziert. Außerdem werden gemäß den in der Dienstbedingungenverwaltungstabelle **1600** umfassten Informationen Dienstbedingungen spezifiziert, die den Dienstbedingungen-IDs **1601** ”2” und ”3” entsprechen. Schließlich wird bestimmt, ob Informationen über eine Zustimmung zu den Dienstbedingungen in den Dienstbedingungen-Zustimmungsinformationen **1205**, die ”Admin1” entsprechen, aufgezeichnet wurden. Da die Zustimmung bei diesem Ausführungsbeispiel vorgenommen wurde, wird in Schritt S2.12 in einen Prozess eingetreten, der durchzuführen ist, wenn Dienstbedingungen nicht existieren, für die es erforderlich ist, dass eine Zustimmung vorgenommen wird. Wenn die Zustimmung zu den Dienstbedingungen nicht vorgenommen wurde, wird in Schritt S2.13 in einen Prozess eingetreten, der durchzuführen ist, wenn Dienstbedingungen existieren, für die es erforderlich ist, dass eine Zustimmung vorgenommen wird. Durch diesen Prozess wird ein Prozess zum Bestimmen abgeschlossen, ob ein Prozess zur Zustimmung zu Dienstbedingungen erforderlich ist, wenn der Benutzer ein Administrator ist. Der Ablauf des detaillierten Prozesses zum Bestimmen, ob Dienstbedingungen existieren, für die es erforderlich ist, dass eine Zustimmung vorgenommen wird, der in Schritt S1.10 durchgeführt wird, wurde hierin vorstehend beschrieben.

[0039] Die Beschreibung kehrt zu dem Prozess beginnend Schritt S1.10 in **Fig.** 6 zurück. Wenn Dienstbedingungen existieren, für die es erforderlich ist, dass eine Zustimmung vorgenommen wird, erzeugt das Dienstbedingungen-Zustimmung-UI-Modul **800** einen Dienstbedingungen-Zustimmungsbildschirm unter Verwendung der Daten des Inhalts **1605**, stellt es die in Schritt S1.4 erzeugte Verschlüsselungssitzung auf ein Cookie ein, und überträgt es eine Antwort an das Clientendgerät **220**. **Fig.** 8A und **Fig.** 8B sind Darstellungen, die die Dienstbedingungen-Zustimmungsbildschirme **8000** und **8010** gemäß diesem Ausführungsbeispiel veranschaulichen. **Fig.** 8A ist eine Darstellung, die ein Beispiel eines Bildschirms veranschaulicht, wenn nur eine Zustimmung zu Dienstbedingungen erforderlich ist. Da das System nicht ohne Vornahme einer Zustimmung zu den Dienstbedingungen verwendet werden darf, kann auf dem Bildschirm nur eine Taste bzw. Schaltfläche bereitgestellt werden, die eine Zustimmung darstellt. Wenn der Benutzer den Dienstbedingungen nicht zustimmen möchte, wird der Prozess durch Schließen bzw. Beenden des Webbrowsers **1000** oder dergleichen beendet. **Fig.** 8B ist eine Darstellung, die ein Beispiel eines Bildschirms veranschaulicht, wenn es erforderlich ist, dass eine Zustimmung zu oder eine Ablehnung von Dienstbedingungen vorgenommen wird. In einem Fall, in dem ein bestimmter Prozess durchzuführen ist (zum Beispiel eine Anzeige einer Nachricht), wenn eine Ablehnung ausgewählt wird, wird dieser Bildschirm verwendet. Ein Prozess, der durchzuführen ist, wenn eine Zustimmung ausgewählt wird, ist gleich demjenigen, der unter Bezugnahme auf **Fig.** 8A beschrieben ist.

[0040] Die Daten von Inhalt **1605** werden in Bereichen **8001** und **8011** angezeigt, und es wird eine Zustimmungstaste bzw. -schaltfläche in Bereichen **8002** und **8012** bereitgestellt. Außerdem wird eine Ablehnungstaste bzw. -schaltfläche in Bereich **8013** bereitgestellt. Wenn eine der Zustimmungstasten bzw. -schaltflächen **8002** und **8012**, die in Dienstbedingungen-Zustimmungsbildschirmen **8000** und **8010** umfasst sind, und der Ablehnungstaste bzw. -schaltfläche **8013**, die in dem Dienstbedingungen-Zustimmungsbildschirm **8010** umfasst ist, gedrückt wird, überträgt der Webbrowser **1000** eine Anforderung zum Benachrichtigen des Webbrowsers

1000 über Zustimmungsinformationen an das Dienstbedingungen-Zustimmung-UI-Modul **800** des Mandantenverwaltungsservers **230**. Hier werden auch Informationen über die Verschlüsselungsinformationen übertragen (S1.12). Das Dienstbedingungen-Zustimmung-UI-Modul **800** erhält Zustimmungsinformationen aus der Anforderung, die von dem Webbrowser **1000** geliefert wird. Wenn die Zustimmung nicht vorgenommen wurde, wird die Verschlüsselungssitzung gelöscht und wird ein Fehlerbildschirm an den Client als Antwort geliefert. Wenn die Zustimmung vorgenommen wurde, wird die Verschlüsselungssitzung aus der Anforderung erhalten und wird ein Entschlüsselungsprozess durchgeführt, um Informationen über die Authentisierungssitzung zu erhalten (S1.13). Das Dienstbedingungen-Zustimmung-UI-Modul **800** überträgt die erhaltene Authentisierungssitzung und eine ID der Dienstbedingungen, die der Zustimmung entsprechen, an das Authentisierungsmodul **610** und stellt die Benutzereigenschaft ein (S1.14).

[0041] Das Authentisierungsmodul **610** spezifiziert einen Benutzer, der der Authentisierungssitzung entspricht, aus den Sitzungsinformationen **1206** der Benutzerverwaltungstabelle **1200** und stellt die ID der Dienstbedingungen auf die Dienstbedingungen-Zustimmungsinformationen **1205** ein. Das Dienstbedingungen-Zustimmung-UI-Modul **800** bestimmt weiterhin, ob Dienstbedingungen existieren, für die es erforderlich ist, dass eine Zustimmung vorgenommen wird, in Schritten S1.15, S1.16 und S1.17. Diese Bestimmung wird durch einen Prozess durchgeführt, der gleich demjenigen in Schritten S1.8, S1.9 und S.10 ist. Wenn in Schritt S1.17 bestimmt wird, dass Dienstbedingungen nicht existieren, für die es erforderlich ist, dass eine Zustimmung vorgenommen wird, stellt das Dienstbedingungen-Zustimmung-UI-Modul **800** eine Authentisierungssitzung auf ein Cookie ein, und benachrichtigt es das Clientendgerät **220** über eine Umlenkung bzw. -schaltung auf einen durch den Ressourcenserver **210** bereitgestellten Webdienst als Antwort (S1.18). Erst nachdem der Benutzer allen Dienstbedingungen zustimmt, kann das Clientendgerät **220** die Authentisierungssitzung von dem Server erhalten. Dadurch wird ein Zugriff auf Webdienste ermöglicht, die die Authentisierungssitzung erfordern, und kann das Clientendgerät **220** eine Verwendung der Webdienste des Informationsverarbeitungsserversystems starten.

[0042] Vorstehend wurde hierin der Ablauf von Prozessen, in denen der Benutzer ein Login von einer Webseite durchführt, Dienstbedingungen zustimmt und eine Verwendung von einem Webdienst startet, gemäß diesem Ausführungsbeispiel beschrieben.

Zweites Ausführungsbeispiel

[0043] Als ein zweites Ausführungsbeispiel wird ein Dienstbedingungen-Zustimmungsverfahren in einer Umgebung beschrieben, in der ein Informationsverarbeitungsserversystem der vorliegenden Offenbarung als ein Dienstanbieter (SP: ”Service Provider”) dient, der einen IdP eines anderen Informationsverarbeitungsserversystems und eine Einmal- bzw. Einzelanmeldung (SSO: ”Single Sign-On”) durch SAML verwirklicht. Es wird angenommen, dass ein Authentisierungsserver **200** und ein IdP **240** alle Einstellungen, die für SSO durch SAML erforderlich sind, im Voraus eingestellt haben. Außerdem ist eine SSO-Hook-Modul **620** so eingestellt, dass es alle Antworten auf einen Zugriff auf Webseiten des Authentisierungsservers **200** verteilt bzw. gabelt/koppelt/schaltet. Die Verteilungs- bzw. Gabelungs-/Kopplungs-/Schaltungseinstellung wird auf einem Webserver durchgeführt, der eine HTTP-Funktion des Authentisierungsservers steuert. Allgemeine Webdienste sind in der Lage, einen Prozess im Verlauf/Zuge eines Prozesses der HTTP-Funktion durch Hinzufügung eines externen Moduls hinzuzufügen. Das SSO-Hook-Modul **620** wird als ein externes Modul erzeugt und in einen Prozess des Webservers eingebunden, der zu einer Zeit durchgeführt wird, wenn alle HTTP-Antworten an ein Clientendgerät **220** zurückgegeben werden.

[0044] Unter Bezugnahme auf **Fig.** 9 wird ein Verfahren für einen Ablauf von Prozessen beschrieben, in denen ein Benutzer ein Login von einer Webseite von dem IdP durchführt, das Clientendgerät **220** mittels SSO von SAML auf das Informationsverarbeitungsserversystem zugreift und ein Anzeigen von einem Bildschirm zur Zustimmung zu Dienstbedingungen durchgeführt wird. Zunächst greift ein Webbrowser **1000** auf ein Login-UI-Modul **900** von dem IdP **240** zu, so dass ein Login durchgeführt wird (S3.1). Das Login-UI-Modul **900** führt einen Login-Prozess durch und erzeugt eine SAML-Antwort. Eine durch einen allgemeinen IdP erzeugte SAML-Antwort umfasst Informationen zum Identifizieren eines authentisierten Benutzers und dergleichen und weist weiterhin eine elektronische Signatur auf. Das Login-UI-Modul **900** überträgt die SAML-Antwort zusammen mit einer Anweisung zur Umlenkung bzw. -schaltung auf das System an das Clientendgerät **220**. Ein Webbrowser **1000** des Clientendgeräts **220** überträgt die SAML-Antwort an ein Authentisierungsmodul **610** eines Authentisierungsservers **200** und überträgt gleichzeitig eine SAML-Verifikationsanforderung an das Authentisierungsmodul **610**. Das Authentisierungsmodul **610** verifiziert, ob die empfangene SAML-Antwort angemessen bzw. sachgemäß ist. In dieser Verifikation wird bestimmt, ob die elektronische Signatur der SAML-Antwort durch den im Voraus eingestellten IdP **240** hinzugefügt wurde, und werden daraufhin in der SAML-Antwort umfasste Informationen zum Identifi-

zieren eines Benutzers erhalten. Außerdem wird gemäß Informationen über eine Abbildung bzw. Zuordnung von einem Benutzer von dem im Voraus eingestellten IdP **240** und einem Benutzer des Informationsverarbeitungsserversystems eine Benutzer-ID, die aus der SAML-Antwort erhalten wird, in eine Benutzer-ID des Benutzers des Informationsverarbeitungsserversystems umgewandelt, so dass ein Login erlaubt wird und eine Authentisierungssitzung bzw. Authentisierungssitzungsinformationen erzeugt wird/werden. Das Authentisierungsmodul **610** speichert die erzeugte Authentisierungssitzung bzw. die erzeugten Authentisierungssitzungsinformationen in Sitzungsinformationen **1206** einer Benutzerverwaltungstabelle **1200** und beabsichtigt daraufhin, eine Antwort an das Clientendgerät **220** zu übertragen (S3.4). Da das SSO-Hook-Modul **620** des Authentisierungsservers **200** alle Antworten von dem Authentisierungsserver **200** verteilt, wird hier auch die Antwort in Schritt S3.4 verteilt. Das SSO-Hook-Modul **620** bestimmt, ob die verteilte Antwort einer SAML-Verifikationserfolgsantwort entspricht (S3.5).

[0045] Unter Bezugnahme auf **Fig.** 10 wird ein detaillierter Ablauf des Prozesses in Schritt S3.5 beschrieben. In Schritt S4.1 wird bestimmt, ob die verteilte Antwort einer Antwort auf eine SAML-Verifikationsanforderung entspricht. Wie es vorstehend beschrieben ist, wird das SSO-Hook-Modul **620** auf Prozessen von allen Antworten von dem Authentisierungsserver **200** ausgeführt und wird daher auch zum Beispiel eine Antwort auf ein Login verteilt. Dementsprechend ist es erforderlich, dass eine Antwort für eine SAML-Verifikation in allen Antworten spezifiziert wird. Das SSO-Hook-Modul **620** speichert eine für die SAML-Verifikation verwendete URL. Unter Verwendung der URL wird bestimmt, ob die verteilte Antwort einer Anforderung von der URL entspricht. Zum Beispiel in einem Fall, in dem das SSO-Hook-Modul **620** eine URL ”/auth/Saml/SP/SSO/Post” für die SAML-Verifikation speichert, wird bestimmt, ob die verteilte Antwort eine Antwort auf eine Anforderung von der URL ist. Wenn ein Abgleich mit der URL in Schritt 4.1 fehlschlägt, schreitet die Verarbeitung zu Schritt S4.4 voran, in dem das SSO-Hook-Modul **620** nichts macht. Wenn der Abgleich mit der URL in Schritt S4.1 erfolgreich durchgeführt wird, schreitet der Prozess zu Schritt S4.2 voran, in dem bestimmt wird, ob ein Cookie der Antwort eine Authentisierungssitzung umfasst. Wenn die SAML-Verifikation erfolgreich durchgeführt wird, wird eine Authentisierungssitzung zum Zugreifen auf das System auf ein Cookie von einer an das Clientendgerät **220** zu liefenden Antwort eingestellt, und wird daher eine Bestimmung dahingehend, ob die SAML-Verifikation erfolgreich durchgeführt wird, durch eine Bestimmung dahingehend vorgenommen, ob die Authentisierungssitzung in dem Cookie umfasst ist. Wenn die SAML-Verifikation fehlschlägt, enthält das Cookie keine Authentisierungssitzung, und schreitet der Prozess daher zu Schritt S4.4 voran. Wenn eine Authentisierungssitzung umfasst ist, schreitet der Prozess zu Schritt S4.3 voran, in dem ein bestimmter Prozess als eine SAML-Verifikationserfolgsantwort durchgeführt wird.

[0046] Das SSO-Hook-Modul **620** führt einen Prozess zur Verschlüsselung der Authentisierungssitzung in Schritt S3.6 von **Fig.** 9 als den bestimmten Prozess der SAML-Verifikationserfolgsantwort durch (S4.3). Ein bei dieser Verschlüsselung verwendeter Verschlüsselungsschlüssel ist gleich demjenigen, der in dem Login-UI-Modul **600** und dem Dienstbedingungen-Zustimmung-UI-Modul **800** verwendet wird. In Schritt S3.6 führt das SSO-Hook-Modul **620** zunächst eine Erlangung und Löschung der Authentisierungssitzung von das Cookie der SAML-Verifikationserfolgsantwort durch. Nachfolgend wird die erlangte Authentisierungssitzung verschlüsselt und auf den Cookie der Antwort eingestellt. Außerdem wird eine URL eines Ziels einer Umlenkung bzw. -schaltung auf einen Webdienst, die erhalten wird, nachdem die SAML-Verifikation erfolgreich durchgeführt ist, die durch den Prozess der SAML-Verifikation eingestellt ist, und die in der Antwort umfasst ist, durch eine URL zur Anzeige eines Dienstbedingungen-Zustimmungsbildschirms ersetzt. Nach dem Prozess in Schritt S3.6 gibt das SSO-Hook-Modul **620** die Antwort an das Clientendgerät **220** zurück (S3.7). Bei Empfang der Anweisung zur Umlenkung bzw. -schaltung überträgt der Webbrowser **1000** eine Anforderung zum Erhalten des Dienstbedingungen-Zustimmungsbildschirms an das Dienstbedingungen-Zustimmung-UI-Modul **800** eines Mandantenverwaltungsservers **230**. Gleichzeitig überträgt der Webbrowser **1000** auch Informationen über die Verschlüsselungssitzung (S3.8).

[0047] Hierin vorstehend wurde der Ablauf von Prozessen beschrieben, in denen der Benutzer einen Login von einer Webseite von dem IdP durchführt und auf das System mittels SSO von SAML zugreift, so dass der Dienstbedingungen-Zustimmungsbildschirm angezeigt wird. Der Prozess beginnend mit Schritt S3.8 ist gleich demjenigen beginnend mit Schritt S1.6 von **Fig.** 6, und eine Verwendung eines Webdiensts kann gestartet werden, nachdem eine Zustimmung zu Dienstbedingungen vorgenommen ist, selbst wenn die SAML-SSO in Kooperation verwendet wird. Demzufolge kann der Benutzer, obwohl das Clientendgerät **220** gemäß dem Stand der Technik eine Umlenkung bzw. -schaltung auf einen Webdienst mittels SAML durchführt, um den Dienst zu empfangen, als Folge eines Zugriffs auf die URL zur Anzeige des Dienstbedingungen-Zustimmungsbildschirms, den Webdienst über das Clientendgerät **220** nur dann verwenden, wenn der Benutzer den Dienstbedingungen zustimmt, und kann der Webdienst dementsprechend sachgemäß bereitgestellt werden.

Drittes Ausführungsbeispiel

[0048] Bei einem dritten Ausführungsbeispiel wird eine Form eines Verfahrens beschrieben, die sich unterscheidet von dem Verfahren zur Verwendung einer Authentisierungssitzung nach Verschlüsselung der Authentisierungssitzung, so dass eine Verschlüsselungssitzung erhalten wird. In diesem Verfahren erzeugt und speichert ein Authentisierungsserver **200** eine mit einer Authentisierungssitzung in Zusammenhang stehende temporäre Sitzung und kann eine Zustimmung zu Dienstbedingungen ohne Verschlüsselung der Authentisierungssitzung vorgenommen werden.

[0049] **Fig.** 11 ist eine Darstellung, die eine Datentabelle veranschaulicht, die in einem externen Speicher durch den Authentisierungsserver **200** gespeichert wird. Anstelle des externen Speichers des Authentisierungsservers **200** kann die Datentabelle in einem anderen Server gespeichert werden, mit dem über das LAN **101** kommuniziert werden kann. Eine Temporärsitzungsverwaltungstabelle **1300** umfasst eine temporäre Sitzung **1301** und eine Authentisierungssitzung **1302**. Die temporäre Sitzung **1301** speichert IDs von temporären Sitzungen, die in einem System eindeutig identifiziert sind.

[0050] Bei dem dritten Ausführungsbeispiel wird der folgende Prozess anstelle des Authentisierungssitzungsverschlüsselungsprozesses in Schritten S1.4 und S3.6 des ersten und des zweiten Ausführungsbeispiels durchgeführt. Zunächst benachrichtigt ein Login-UI-Modul **600** oder ein SSO-Hook-Modul **620** den Authentisierungsserver **200** über eine Authentisierungssitzung, wenn der Prozess in Schritt S1.4 oder Schritt S3.6 durchgeführt wird, um so eine Erzeugung einer temporären Sitzung anzufordern. Der Authentisierungsserver **200**, der die Anforderung empfangen hat, erzeugt eine temporäre Sitzung, bringt die temporäre Sitzung mit Informationen über die Authentisierungssitzung in Zusammenhang, speichert die Daten in der Temporärsitzungsverwaltungstabelle **1300**, und überträgt die temporäre Sitzung als Antwort. Das Login-UI-Modul **600** oder das SSO-Hook-Modul **620**, das die temporäre Sitzung empfangen hat, verwendet daraufhin die temporäre Sitzung anstelle einer Verschlüsselungssitzung. Als Nächstes wird der folgende Prozess anstelle des Verschlüsselungssitzungsentschlüsselungsprozesses durchgeführt, der in Schritt S1.7 und Schritt S1.13 des ersten Ausführungsbeispiels oder des zweiten Ausführungsbeispiels durchgeführt wird. Ein Dienstbedingungen-Zustimmung-UI-Modul **800** benachrichtigt den Authentisierungsserver **200** über die temporäre Sitzung, wenn der Prozess in Schritt S1.7 und Schritt S1.13 durchgeführt wird, und fordert ein Erhalten einer Authentisierungssitzung an. Der Authentisierungsserver **200**, der die Anforderung empfangen hat, erhält eine der empfangenen temporären Sitzung entsprechende Authentisierungssitzung aus der Temporärsitzungsverwaltungstabelle **1300** und überträgt die Authentisierungssitzung als Antwort. Das Dienstbedingungen-Zustimmung-UI-Modul **800**, das die Authentisierungssitzung empfangen hat, verwendet daraufhin die aus der temporären Sitzung erhaltene Authentisierungssitzung anstelle einer entschlüsselten Authentisierungssitzung. Vorstehend wurde hierin das Verfahren beschrieben, das sich unterscheidet von dem Verfahren zur Verwendung einer Authentisierungssitzung nach Verschlüsselung der Authentisierungssitzung, so dass eine Verschlüsselungssitzung erhalten wird.

[0051] Es ist ein Informationsverarbeitungsserversystem bereitgestellt, das der Lage ist, unter Verwendung einer Authentisierungssitzung, die sich von einer Authentisierungssitzung unterscheidet, die von einem Client zur Verwendung eines Webdiensts verwendet wird, zu bestimmen, dass ein Benutzer Dienstbedingungen zustimmt.

Weitere Ausführungsbeispiele

[0052] Zusätzliche Ausführungsbeispiele können auch verwirklicht werden durch einen Computer eines Systems oder einer Vorrichtung, der computerausführbare Anweisungen, die auf einem Speichermedium (z. B. einem computerlesbaren Speichermedium) aufgezeichnet sind, ausliest und ausführt, um die Funktionen von einem oder mehreren der vorstehend beschriebenen Ausführungsbeispiele durchzuführen, sowie durch ein Verfahren, dass durch den Computer des Systems oder der Vorrichtung durchgeführt wird, indem zum Beispiel die computerausführbaren Anweisungen von dem Speichermedium ausgelesen und ausgeführt werden, um die Funktionen von einem oder mehreren der vorstehend beschriebenen Ausführungsbeispiele durchzuführen. Der Computer kann eine oder mehrere von einer zentralen Verarbeitungseinheit (CPU), einer Mikroverarbeitungseinheit (MPU) oder einer Schaltung aufweisen, und er kann ein Netzwerk separater Computer oder separater Computerprozessoren umfassen. Die computerausführbaren Anweisungen können an den Computer zum Beispiel von einem Netzwerk oder dem Speichermedium bereitgestellt werden. Das Speichermedium kann zum Beispiel eines oder mehreres von einer Festplatte, einem Direktgriffsspeicher (RAM), einem Festwertspeicher (ROM), einem Speicher von verteilten Rechensystemen, 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.

[0053] Während die vorliegende Offenbarung unter Bezugnahme auf beispielhafte Ausführungsbeispiele beschrieben wurde, ist es selbstverständlich, dass diese beispielhaften Ausführungsbeispiele nicht als

einschränkend verstanden werden. Dem Umfang der folgenden Patentansprüche ist die breiteste Auslegung zuzugestehen, um alle derartigen Modifikationen und äquivalente Strukturen und Funktionen zu umfassen.

[0054] Es ist ein Informationsverarbeitungsserversystem bereitgestellt, in dem eine Zustimmung zu Dienstbedingungen durch einen Benutzer unter Verwendung einer zweiten Authentisierungssitzung bestätigt wird, die sich von einer ersten Authentisierungssitzung unterscheidet, die verwendet wird, wenn ein Client den Webdienst verwendet.

ZITATE ENTHALTEN IN DER BESCHREIBUNG

Diese Liste der vom Anmelder aufgeführten Dokumente wurde automatisiert erzeugt und ist ausschließlich zur besseren Information des Lesers aufgenommen. Die Liste ist nicht Bestandteil der deutschen Patent- bzw. Gebrauchsmusteranmeldung. Das DPMA übernimmt keinerlei Haftung für etwaige Fehler oder Auslassungen.

Zitierte Patentliteratur

- JP 4056390 [0005]

Patentansprüche

1. Informationsverarbeitungsserversystem mit:
einer Erzeugungseinrichtung zum Erzeugen einer zweiten Authentisierungssitzung basierend auf einer ersten Authentisierungssitzung, die erzeugt wird, nachdem ein Benutzer authentisiert ist, und die verwendet wird, wenn ein Client einen Webdienst verwendet;
einer Übertragungseinrichtung zum Übertragen der zweiten Authentisierungssitzung an den Client; und
einer Empfangseinrichtung zum Empfangen der zweiten Authentisierungssitzung zusammen mit Informationen, die eine Zustimmung zu Bedingungen des Webdiensts darstellen, von dem Client,
wobei die Übertragungseinrichtung die erste Authentisierungssitzung, die der zweiten Authentisierungssitzung entspricht, an den Client überträgt, wenn gemäß den empfangenen Informationen und der zweiten Authentisierungssitzung bestimmt wird, dass der Benutzer den Bedingungen des Webdiensts zugestimmt hat.

2. Informationsverarbeitungsserversystem gemäß Anspruch 1, zusätzlich mit:
einer Verteilungseinrichtung zum Verteilen der ersten Authentisierungssitzung, die an den Client von einem Authentisierungsserver zu übertragen ist, der eine Antwort empfängt, die darstellt, dass der Benutzer durch ein andere Informationsverarbeitungsserversystem authentisiert wurde, in Erwiderung auf den Empfang der Antwort,
wobei die Erzeugungseinrichtung die zweite Authentisierungssitzung basierend auf der durch die Verteilungseinrichtung verteilten ersten Authentisierungssitzung erzeugt.

3. Informationsverarbeitungsserversystem gemäß Anspruch 1, zusätzlich mit:
einer Bereitstellungseinrichtung zum Bereitstellen eines Bildschirms zur Zustimmung zu den Bedingungen des Webdiensts oder einer Vielzahl von Bildschirmen zur Zustimmung zu Bedingungen von Webdiensten, die für einen authentisierten Benutzer verfügbar sind,
wobei die Übertragungsseinrichtung die erste Authentisierungssitzung, die der zweiten Authentisierungssitzung entspricht, an den Client überträgt, wenn bestimmt wird, dass der authentisierte Benutzer allen Bedingungen von Webdiensten zugestimmt hat, die für den authentisierten Benutzer verfügbar sind.

4. Informationsverarbeitungsserversystem gemäß Anspruch 3, wobei die Bereitstellungseinrichtung einen Bildschirm zur Zustimmung zu Bedingungen des Webdiensts bereitstellt, der mit einem Mandanten des Benutzers in Zusammenhang steht, wenn für den authentisierten Benutzer kein Webdienst verfügbar ist.

5. Informationsverarbeitungsserversystem gemäß Anspruch 1, wobei
die Erzeugungseinrichtung die zweite Authentisierungssitzung durch Verschlüsselung der ersten Authentisierungssitzung erzeugt, und
die Übertragungseinrichtung die durch die Empfangseinrichtung empfangene zweite Authentisierungssitzung entschlüsselt und die durch die Entschlüsselung erhaltene erste Authentisierungssitzung an den Client überträgt.

6. Verfahren zur Steuerung eines Informationsverarbeitungsserversystems, mit:
einem Schritt des Erzeugens einer zweiten Authentisierungssitzung basierend auf einer ersten Authentisierungssitzung, die erzeugt wird, nachdem ein Benutzer authentisiert ist, und die verwendet wird, wenn ein Client einen Webdienst verwendet;
einen Schritt des Übertragens der zweiten Authentisierungssitzung an den Client; und
einen Schritt des Empfangens der zweiten Authentisierungssitzung zusammen mit Informationen, die eine Zustimmung zu Bedingungen des Webdiensts darstellen, von dem Client,
wobei die erste Authentisierungssitzung, die der zweiten Authentisierungssitzung entspricht, an den Client übertragen wird, wenn gemäß den empfangenen Informationen und der zweiten Authentisierungssitzung bestimmt wird, dass der Benutzer den Bedingungen des Webdiensts zugestimmt hat.

7. Verfahren gemäß Anspruch 6, zusätzlich mit:
einem Schritt des Verteilens der ersten Authentisierungssitzung, die an den Client von einem Authentisierungsserver zu übertragen ist, der eine Antwort empfängt, die darstellt, dass der Benutzer durch ein anderes Informationsverarbeitungsserversystem authentisiert wurde, in Erwiderung auf dien Empfang der Antwort,
wobei die zweite Authentisierungssitzung basierend auf der in dem Verteilungsschritt verteilten ersten Authentisierungssitzung erzeugt wird.

8. Verfahren gemäß Anspruch 6, zusätzlich mit:
einem Schritt des Bereitstellens eines Bildschirms zur Zustimmung zu den Bedingungen des Webdiensts oder einer Vielzahl von Bildschirmen zur Zustimmung zu Bedingungen von Webdiensten, die für einen authentisierten Benutzer verfügbar sind,
wobei die erste Authentisierungssitzung, die der zweiten Authentisierungssitzung entspricht, an den Client übertragen wird, wenn bestimmt wird, dass der authentisierte Benutzer allen Bedingungen von Webdiensten zugestimmt hat, die für den authentisierten Benutzer verfügbar sind.

9. Verfahren gemäß Anspruch 8, wobei ein Bildschirm zur Zustimmung zu Bedingungen des Webdiensts, der mit einem Mandanten des Benutzers in Zusammenhang steht, bereitgestellt wird, wenn für

den authentisierten Benutzer kein Webdienst verfügbar ist.

10. Verfahren gemäß Anspruch 6, wobei
die zweite Authentisierungssitzung durch Verschlüsselung der ersten Authentisierungssitzung erzeugt wird, und
die zweite Authentisierungssitzung entschlüsselt wird und die durch die Entschlüsselung erhaltene erste Authentisierungssitzung an den Client übertragen wird.

11. Programm, das einen Computer veranlasst, das Verfahren gemäß Anspruch 6 auszuführen.

Es folgen 11 Seiten Zeichnungen

Anhängende Zeichnungen

FIG. 1

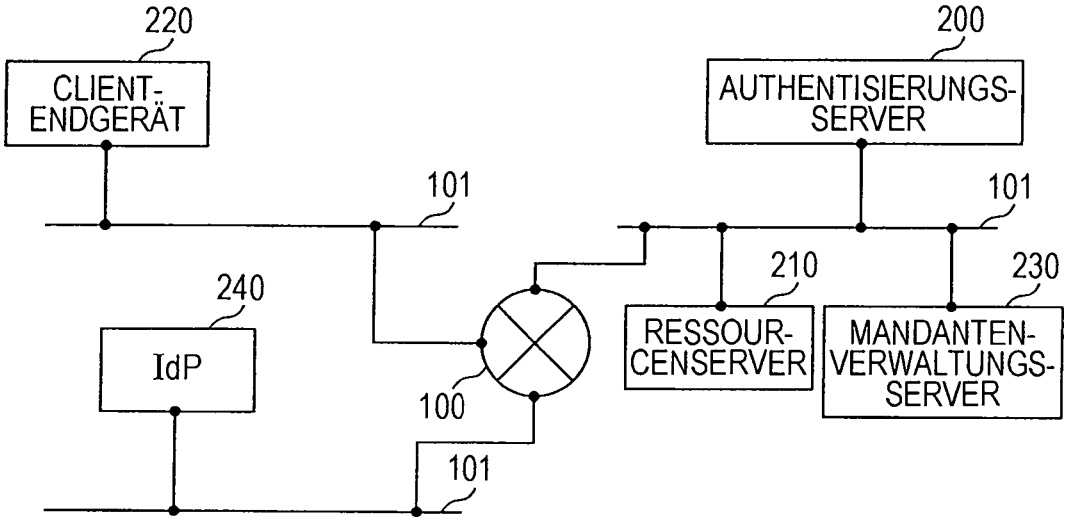


FIG. 2

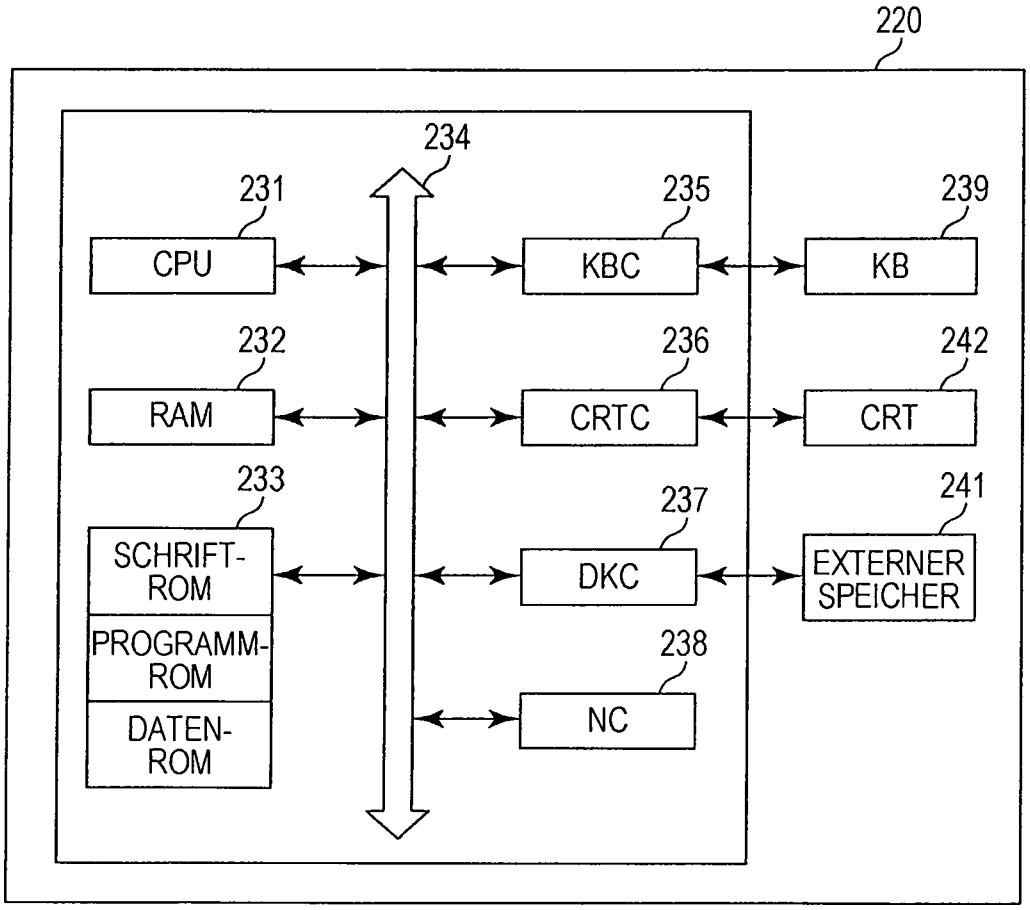

220
234
231
CPU
235
KBC
239
KB
232
RAM
236
CRTC
242
CRT
233
SCHRIFT-ROM
PROGRAMM-ROM
DATEN-ROM
237
DKC
241
EXTERNER SPEICHER
238
NC

FIG. 3

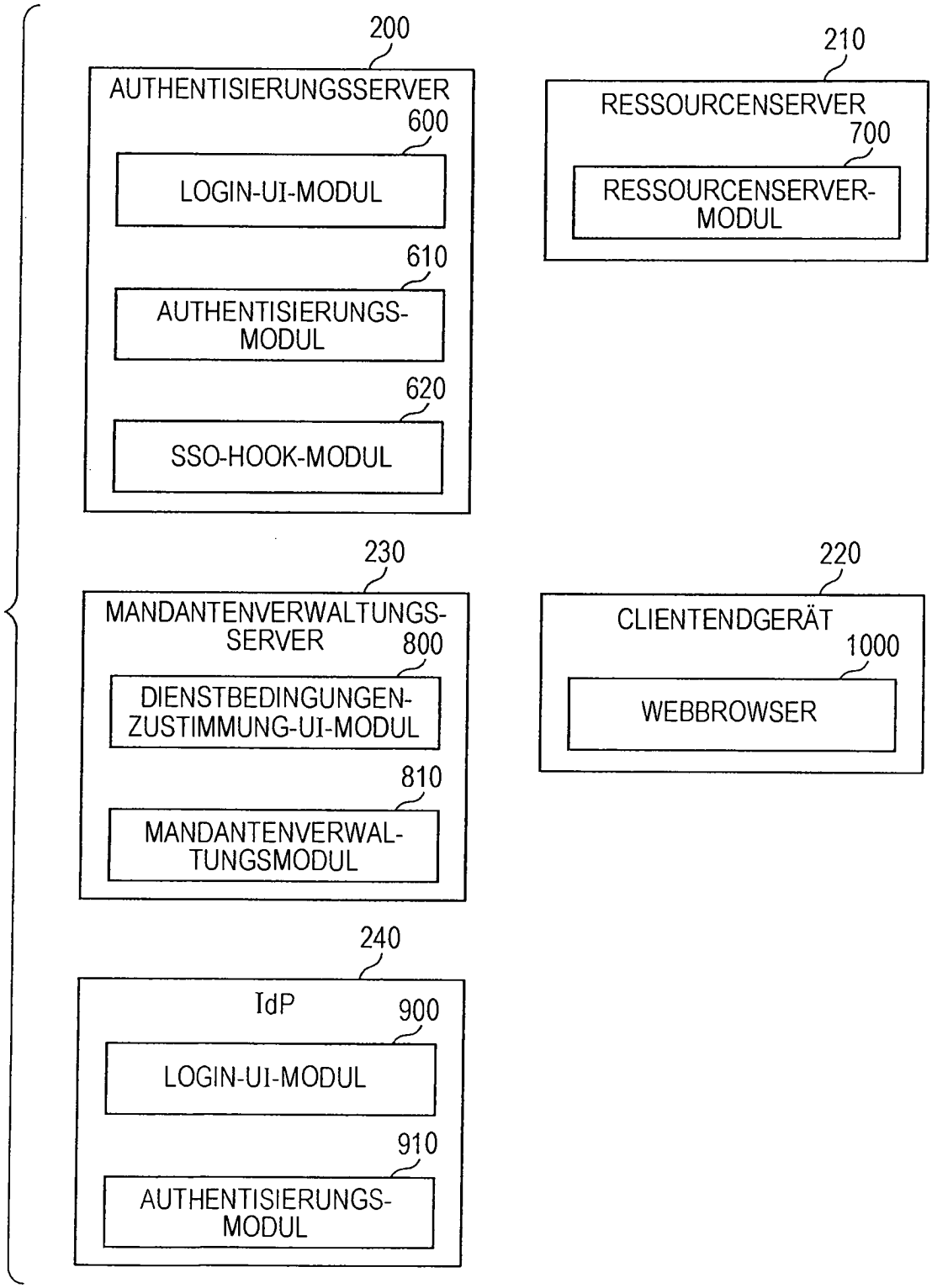

200
AUTHENTISIERUNGSSERVER
600
LOGIN-UI-MODUL
610
AUTHENTISIERUNGS-MODUL
620
SSO-HOOK-MODUL
210
RESSOURCENSERVER
700
RESSOURCENSERVER-MODUL
230
MANDANTENVERWALTUNGS-SERVER
800
DIENSTBEDINGUNGEN-ZUSTIMMUNG-UI-MODUL
810
MANDANTENVERWAL-TUNGSMODUL
220
CLIENTENDGERÄT
1000
WEBBROWSER
240
IdP
900
LOGIN-UI-MODUL
910
AUTHENTISIERUNGS-MODUL

FIG. 4

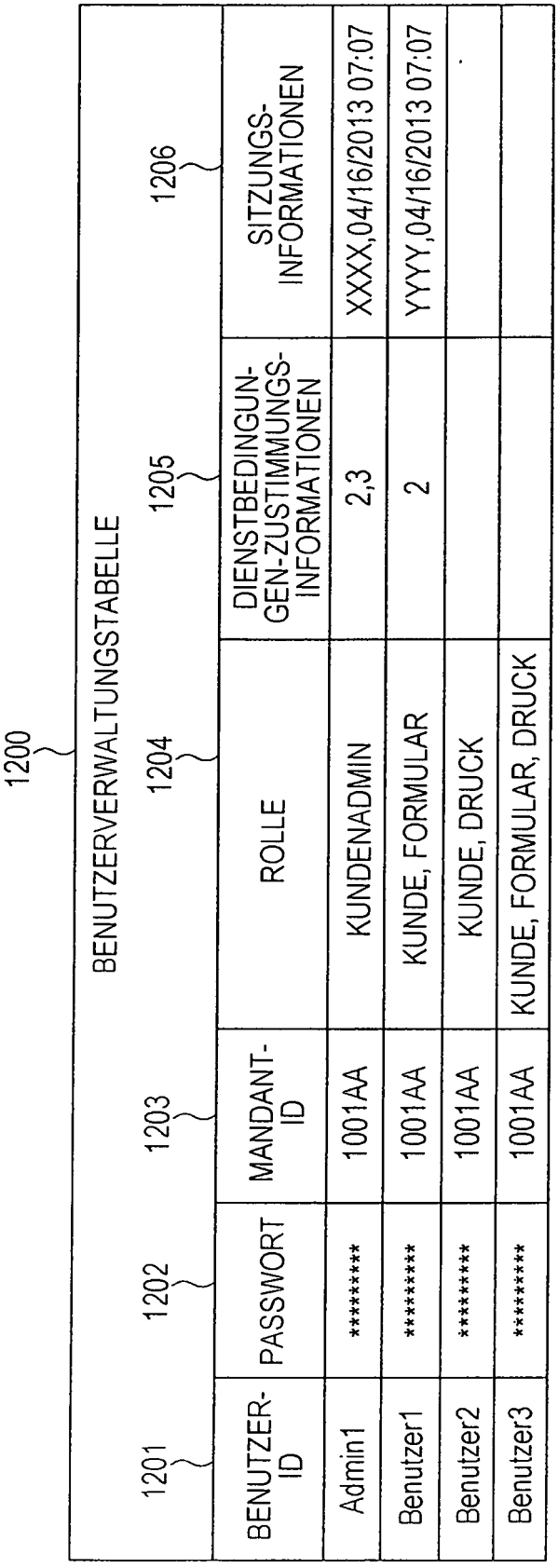

1200
BENUTZERVERWALTUNGSTABELLE
1201
1202
1203
1204
1205
1206
BENUTZER-ID
PASSWORT
MANDANT-ID
ROLLE
DIENSTBEDINGUN-GEN-ZUSTIMMUNGS-INFORMATIONEN
SITZUNGS-INFORMATIONEN
Admin1
****
1001AA
KUNDENADMIN
2,3
XXXX,04/16/2013 07:07
Benutzer1
****
1001AA
KUNDE, FORMULAR
2
YYYY,04/16/2013 07:07
Benutzer2
****
1001AA
KUNDE, DRUCK
Benutzer3
****
1001AA
KUNDE, FORMULAR, DRUCK

FIG. 5A

1500

LIZENZTABELLE

1501 MANDANT-ID	1502 VERKAUFS-MANDANT-ID	1503 LIZENZ	1504 LIZENZ-ZÄHLUNG
1001AA	101AA	FORMULAR	20
1001AA	101AA	DRUCK	20

FIG. 5B

1600

DIENSTBEDINGUNGENVERWALTUNGSTABELLE

1601 DIENSTBEDINGUNGEN-ID	1602 VERKAUFS-MANDANT-ID	1603 LIZENZ	1604 ÄNDERUNG	1605 INHALT
1	101AA	FORMULAR	1	ZUSTIMMUNG ZU FORMULARDIENSTBEDINGUNGEN XX...
2	101AA	FORMULAR	2	ZUSTIMMUNG ZU FORMULARDIENSTBEDINGUNGEN XX...
3	101AA	DRUCK	1	DRUCKDIENSTBEDINGUNGEN ZZ. ZUSTIMMUNG ZU XX...
4	102AA	FORMULAR, DRUCK	1	FORMULAR-/DRUCKDIENSTBEDINGUNGEN. ZUSTIMMUNG ZU XX...

FIG. 6

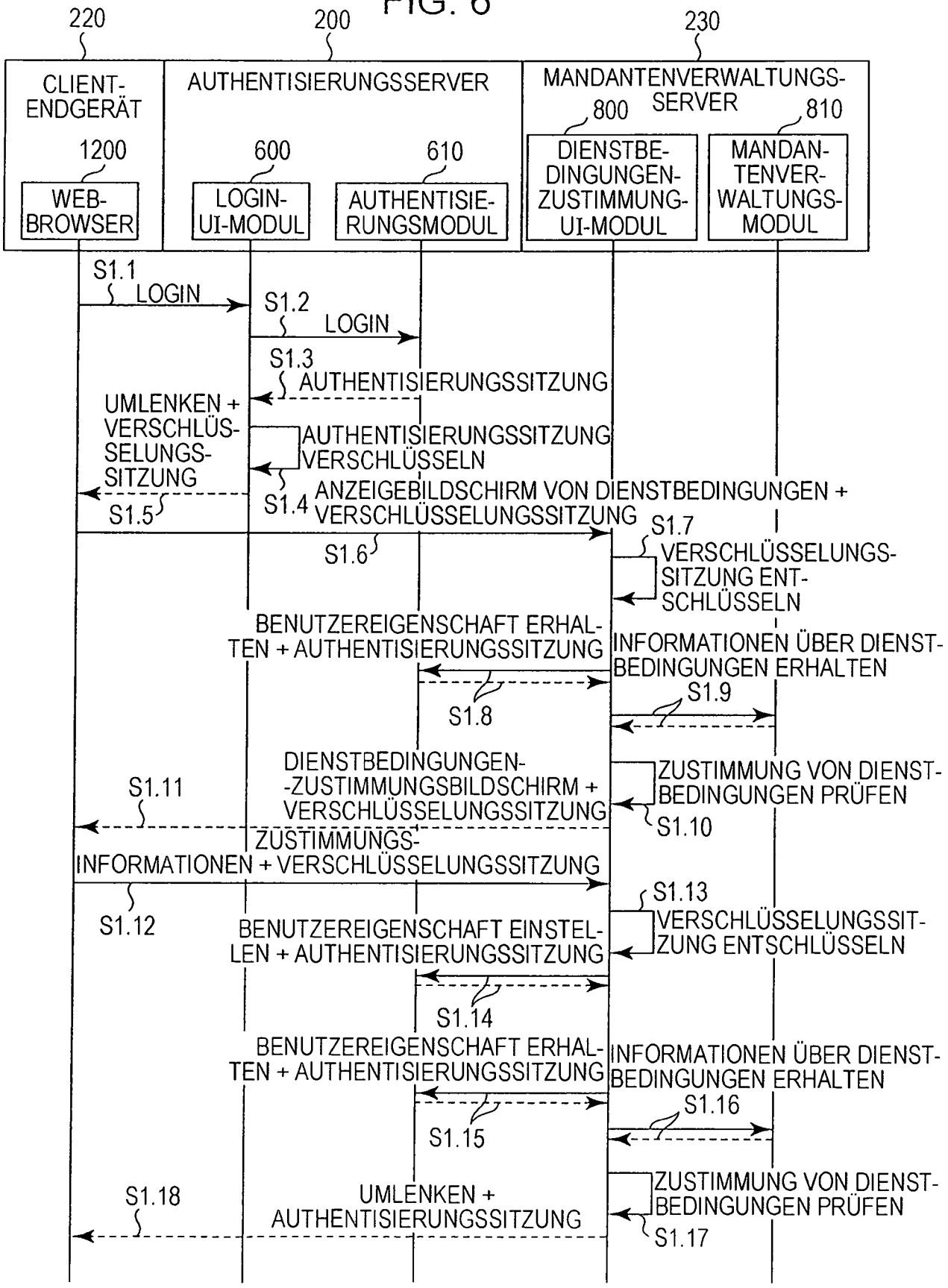

220
200
230
CLIENT-ENDGERÄT
AUTHENTISIERUNGSSERVER
MANDANTENVERWALTUNGS-SERVER
800
810
1200
600
610
WEB-BROWSER
LOGIN-UI-MODUL
AUTHENTISIE-RUNGSMODUL
DIENSTBE-DINGUNGEN-ZUSTIMMUNG-UI-MODUL
MANDAN-TENVER-WALTUNGS-MODUL
S1.1
LOGIN
S1.2
LOGIN
S1.3
AUTHENTISIERUNGSSITZUNG
UMLENKEN + VERSCHLÜS-SELUNGS-SITZUNG
AUTHENTISIERUNGSSITZUNG VERSCHLÜSSELN
S1.4
S1.5
ANZEIGEBILDSCHIRM VON DIENSTBEDINGUNGEN + VERSCHLÜSSELUNGSSITZUNG
S1.6
S1.7
VERSCHLÜSSELUNGS-SITZUNG ENT-SCHLÜSSELN
BENUTZEREIGENSCHAFT ERHAL-TEN + AUTHENTISIERUNGSSITZUNG
INFORMATIONEN ÜBER DIENST-BEDINGUNGEN ERHALTEN
S1.8
S1.9
DIENSTBEDINGUNGEN--ZUSTIMMUNGSBILDSCHIRM + VERSCHLÜSSELUNGSSITZUNG
ZUSTIMMUNG VON DIENST-BEDINGUNGEN PRÜFEN
S1.11
S1.10
ZUSTIMMUNGS-INFORMATIONEN + VERSCHLÜSSELUNGSSITZUNG
S1.12
S1.13
BENUTZEREIGENSCHAFT EINSTEL-LEN + AUTHENTISIERUNGSSITZUNG
VERSCHLÜSSELUNGSSIT-ZUNG ENTSCHLÜSSELN
S1.14
BENUTZEREIGENSCHAFT ERHAL-TEN + AUTHENTISIERUNGSSITZUNG
INFORMATIONEN ÜBER DIENST-BEDINGUNGEN ERHALTEN
S1.15
S1.16
ZUSTIMMUNG VON DIENST-BEDINGUNGEN PRÜFEN
S1.18
UMLENKEN + AUTHENTISIERUNGSSITZUNG
S1.17

FIG. 7

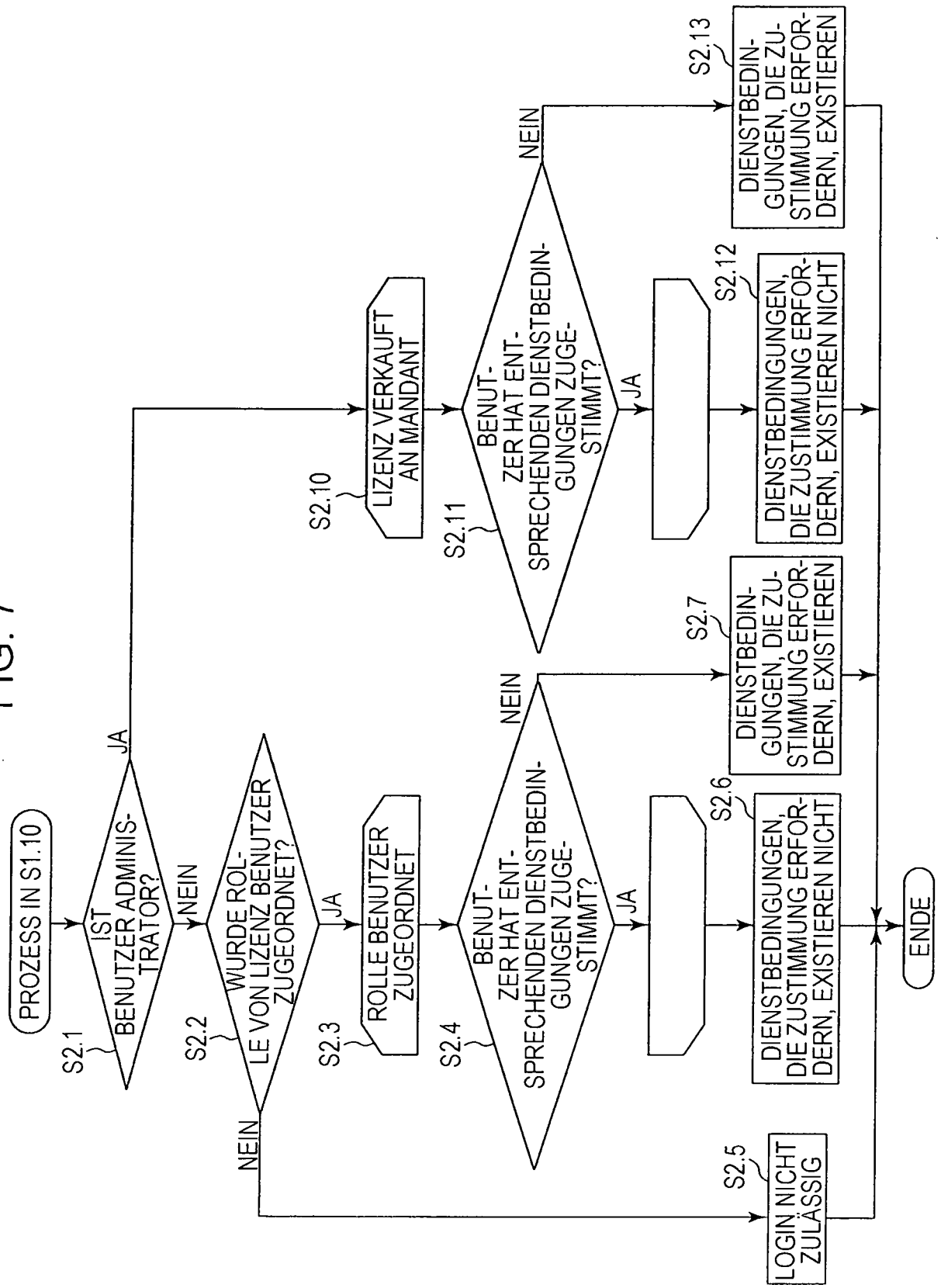

PROZESS IN S1.10
S2.1
IST BENUTZER ADMINISTRATOR?
JA
NEIN
S2.2
WURDE ROLLE VON LIZENZ BENUTZER ZUGEORDNET?
JA
NEIN
S2.3
ROLLE BENUTZER ZUGEORDNET
S2.4
BENUTZER HAT ENTSPRECHENDEN DIENSTBEDINGUNGEN ZUGESTIMMT?
JA
NEIN
S2.5
LOGIN NICHT ZULÄSSIG
S2.6
DIENSTBEDINGUNGEN, DIE ZUSTIMMUNG ERFORDERN, EXISTIEREN NICHT
S2.7
DIENSTBEDINGUNGEN, DIE ZUSTIMMUNG ERFORDERN, EXISTIEREN
S2.10
LIZENZ VERKAUFT AN MANDANT
S2.11
BENUTZER HAT ENTSPRECHENDEN DIENSTBEDINGUNGEN ZUGESTIMMT?
JA
NEIN
S2.12
DIENSTBEDINGUNGEN, DIE ZUSTIMMUNG ERFORDERN, EXISTIEREN NICHT
S2.13
DIENSTBEDINGUNGEN, DIE ZUSTIMMUNG ERFORDERN, EXISTIEREN
ENDE

FIG. 8A

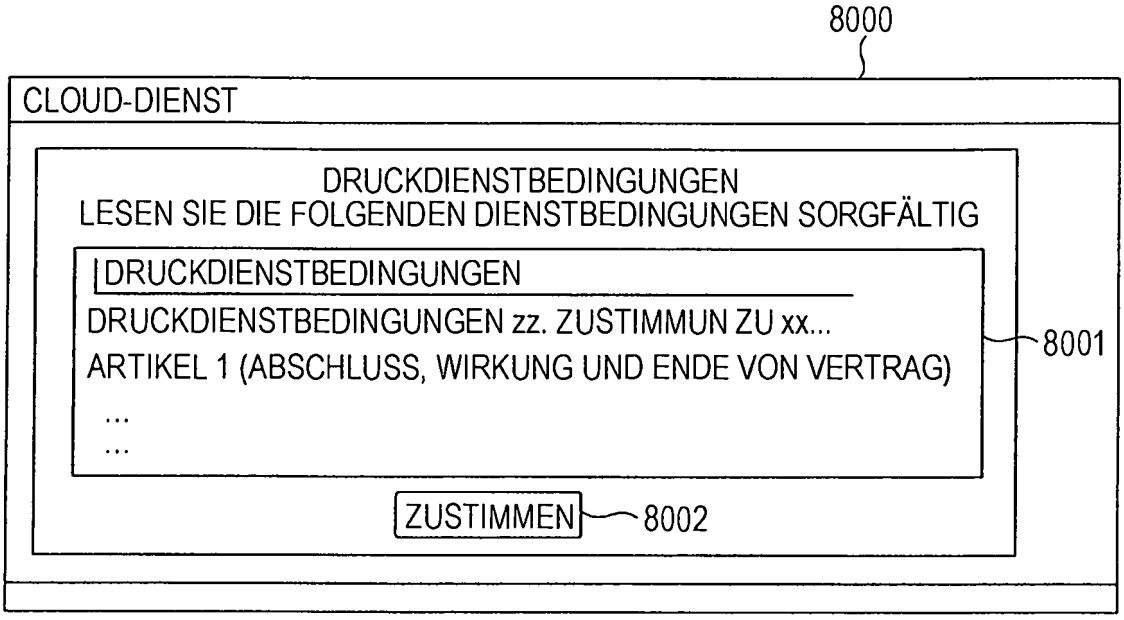

8000
CLOUD-DIENST
DRUCKDIENSTBEDINGUNGEN
LESEN SIE DIE FOLGENDEN DIENSTBEDINGUNGEN SORGFÄLTIG
DRUCKDIENSTBEDINGUNGEN
DRUCKDIENSTBEDINGUNGEN zz. ZUSTIMMUN ZU xx...
ARTIKEL 1 (ABSCHLUSS, WIRKUNG UND ENDE VON VERTRAG)
...
...
8001
ZUSTIMMEN
8002

FIG. 8B

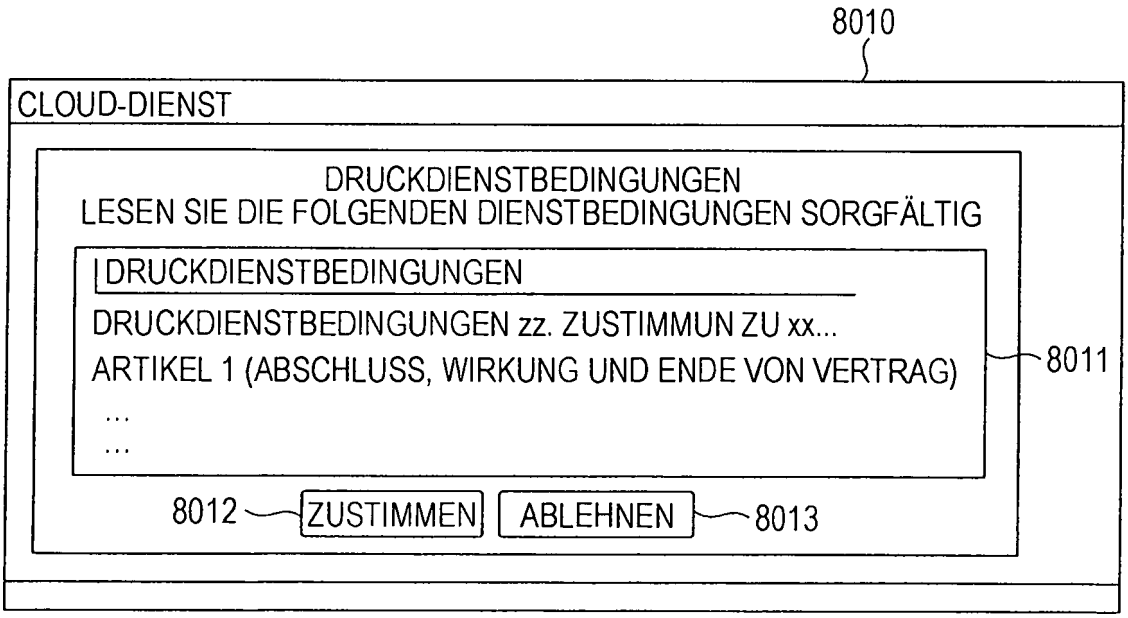

8010
CLOUD-DIENST
DRUCKDIENSTBEDINGUNGEN
LESEN SIE DIE FOLGENDEN DIENSTBEDINGUNGEN SORGFÄLTIG
DRUCKDIENSTBEDINGUNGEN
DRUCKDIENSTBEDINGUNGEN zz. ZUSTIMMUN ZU xx...
ARTIKEL 1 (ABSCHLUSS, WIRKUNG UND ENDE VON VERTRAG)
...
...
8011
8012
ZUSTIMMEN
ABLEHNEN
8013

FIG. 9

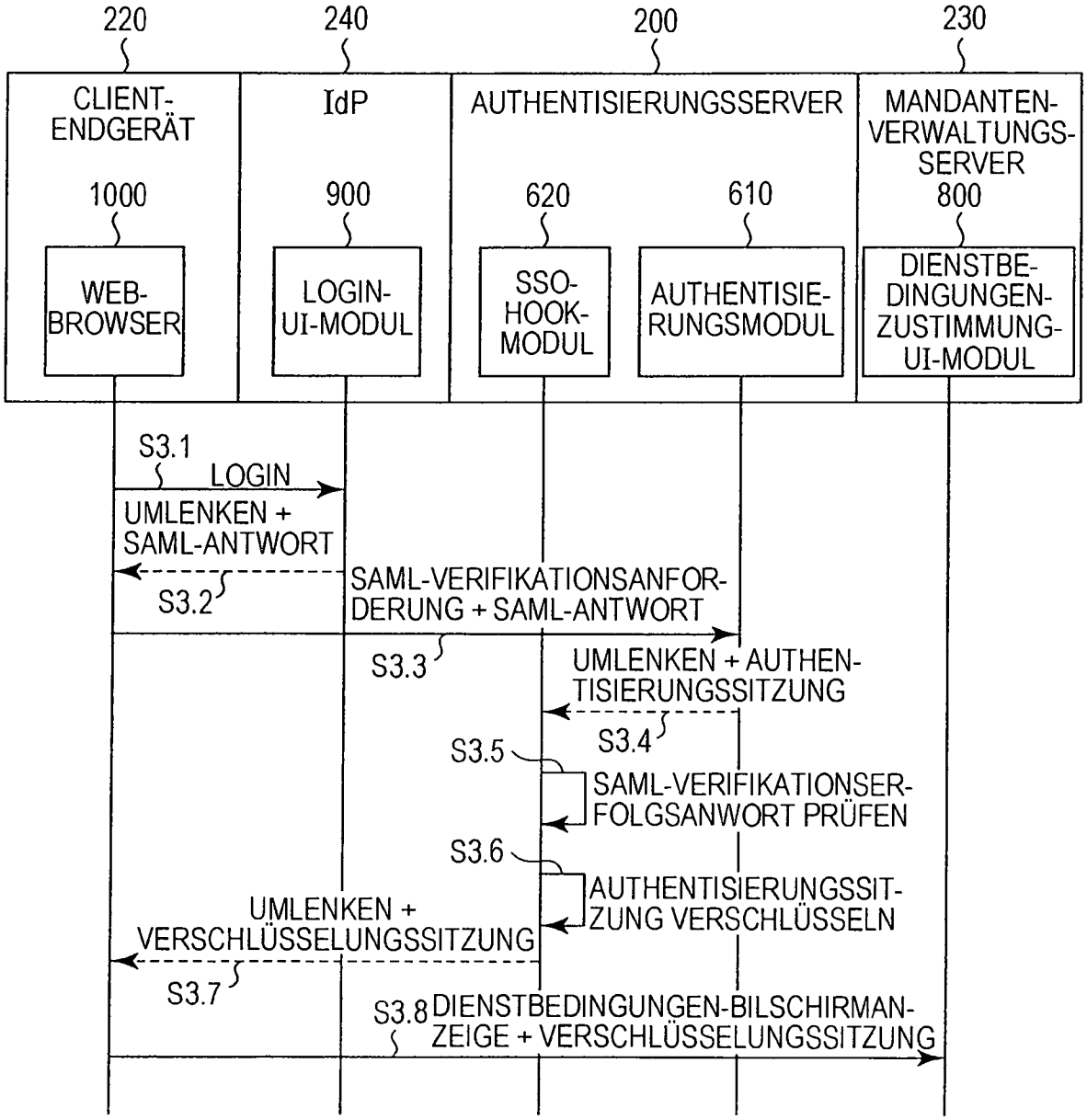

220
240
200
230
CLIENT-ENDGERÄT
IdP
AUTHENTISIERUNGSSERVER
MANDANTEN-VERWALTUNGS-SERVER
1000
900
620
610
800
WEB-BROWSER
LOGIN-UI-MODUL
SSO-HOOK-MODUL
AUTHENTISIE-RUNGSMODUL
DIENSTBE-DINGUNGEN-ZUSTIMMUNG-UI-MODUL
S3.1
LOGIN
UMLENKEN + SAML-ANTWORT
S3.2
SAML-VERIFIKATIONSANFOR-DERUNG + SAML-ANTWORT
S3.3
UMLENKEN + AUTHEN-TISIERUNGSSITZUNG
S3.4
S3.5
SAML-VERIFIKATIONSER-FOLGSANWORT PRÜFEN
S3.6
AUTHENTISIERUNGSSIT-ZUNG VERSCHLÜSSELN
UMLENKEN + VERSCHLÜSSELUNGSSITZUNG
S3.7
S3.8
DIENSTBEDINGUNGEN-BILSCHIRMAN-ZEIGE + VERSCHLÜSSELUNGSSITZUNG

FIG. 10

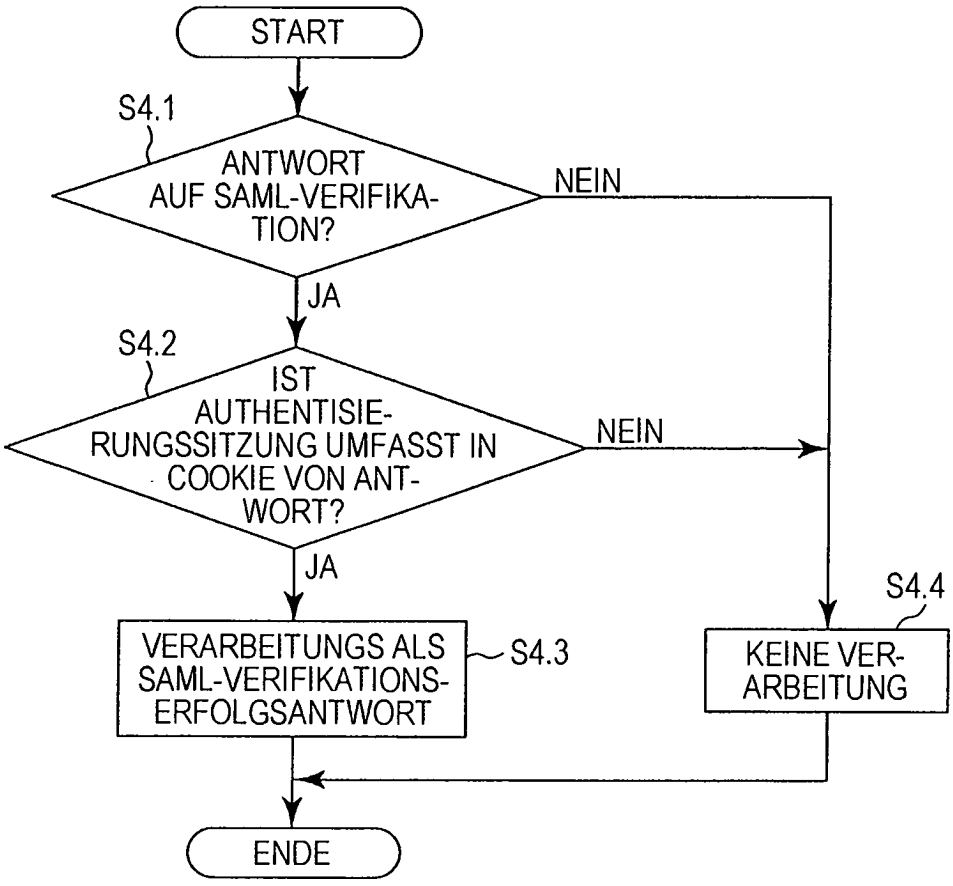
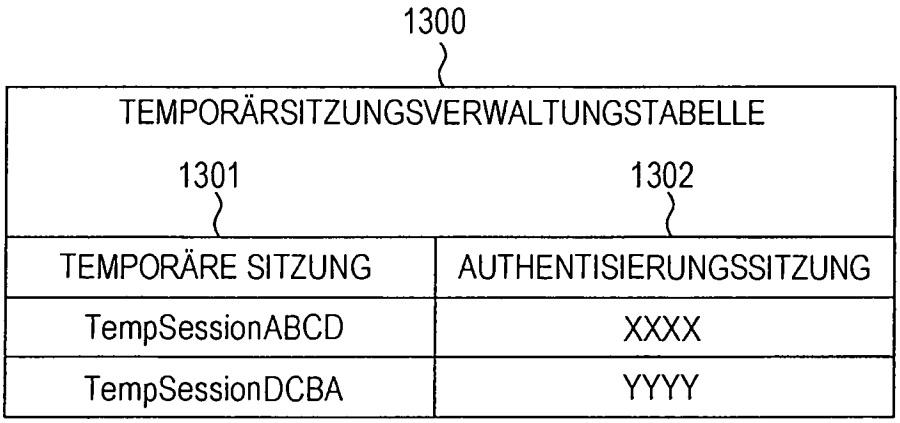

START
S4.1
ANTWORT AUF SAML-VERIFIKA-TION?
NEIN
JA
S4.2
IST AUTHENTISIE-RUNGSSITZUNG UMFASST IN COOKIE VON ANT-WORT?
NEIN
JA
S4.4
VERARBEITUNGS ALS SAML-VERIFIKATIONS-ERFOLGSANTWORT
S4.3
KEINE VER-ARBEITUNG
ENDE

FIG. 11


1300
TEMPORÄRSITZUNGSVERWALTUNGSTABELLE
1301
1302
TEMPORÄRE SITZUNG
AUTHENTISIERUNGSSITZUNG
TempSessionABCD
XXXX
TempSessionDCBA
YYYY