(19) Deutsches Patent- und Markenamt

(10) **DE 10 2017 012 249 A1** 2019.03.21

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2017 012 249.0**
(22) Anmeldetag: **19.09.2017**
(43) Offenlegungstag: **21.03.2019**

(51) Int Cl.: ***H04L 9/32*** (2006.01)
G06F 21/31 (2013.01)

(62) Teilung aus:
10 2017 121 648.0

(71) Anmelder:
APIIDA AG, 64401 Groß-Bieberau, DE

(74) Vertreter:
TER MEER STEINMEISTER & PARTNER PATENTANWÄLTE mbB, 80335 München, DE

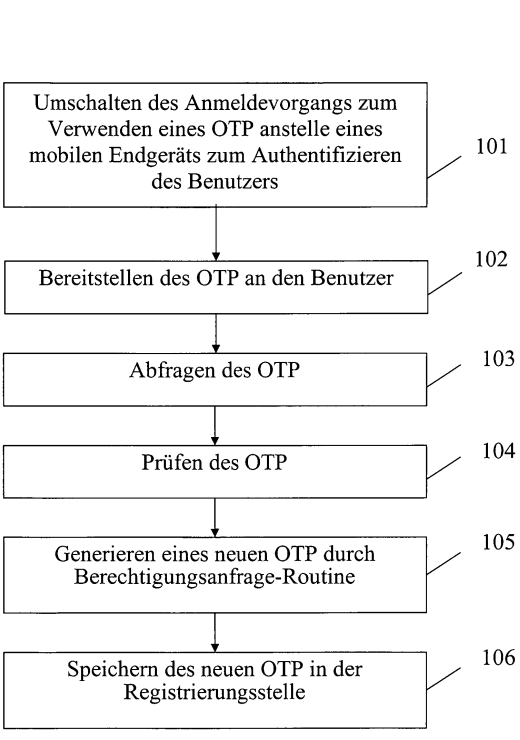
(72) Erfinder:
Müller, Markus, 64401 Groß-Bieberau, DE; Ertl, Frank, 64753 Brombachtal, DE

Prüfungsantrag gemäß § 44 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **Mobiles Endgerät und Verfahren zum Authentifizieren eines Benutzers an einem Endgerät mittels mobilem Endgerät**

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren (100) zum Anmelden eines Benutzers an einem Endgerät (1) mittels eines Einmal-Passworts bei Nichtvorhandensein eines zum Authentifizieren des Benutzers zu verwendenden mobilen Endgeräts (2), wobei das Verfahren (100) die folgenden Schritte umfasst: Umschalten (101) des Anmeldevorgangs am Endgerät (1) zum Verwenden eines Einmal-Passworts anstelle einer Authentifizierung mittels des mobilen Endgeräts (2) zum Authentifizieren dieses Benutzers an diesem Endgerät (1), wobei das Einmal-Passwort bei einer vormaligen Authentifizierung des Benutzers erzeugt wurde und in einer Registrierungsstelle gespeichert ist; Bereitstellen (102) des Einmal-Passworts an den Benutzer; Abfragen (103) des Einmal-Passworts zum Anmelden mittels einer Berechtigungsanfrage-Routine (9) des Endgeräts (1) und Übertragen des eingegebenen Einmal-Passworts mittels der Berechtigungsanfrage-Routine (9) des Endgeräts (1) ; Prüfen (104) des Einmal-Passworts und Authentifizieren des Benutzers an dem Endgerät (1); Generieren (105) eines neuen Einmal-Passworts durch die Berechtigungsanfrage-Routine (9) des Endgeräts (1); und Speichern (106) des neuen Einmal-Passworts in der Registrierungsstelle anstelle des bisherigen Einmal-Passworts und Verwenden des neuen Einmal-Passworts bei einem darauffolgenden Anmelden des Benutzers am Endgeräts (1) bei erneutem Nichtvorhandensein des zum Authentifizieren des Benutzers zu verwendenden mobilen Endgeräts (2). Die Erfindung ...



Beschreibung

TECHNISCHES GEBIET DER ERFINDUNG

[0001] Die Erfindung betrifft ein Verfahren zum Anmelden eines Benutzers an einem digitalen Endgerät. Dabei betrifft die Erfindung ein Verfahren zum Authentifizieren des Benutzers an dem Endgerät. Insbesondere ist die Erfindung auf ein Verfahren zum Anmelden eines Benutzers in einem Netzwerk mittels eines Einmal-Passworts bei Nichtvorhandensein eines zum Authentifizieren des Benutzers verwendeten mobilen Endgeräts gerichtet. Die Erfindung umfasst zudem ein mobiles Endgerät und zwei verschiedene Computerprogrammprodukte.

HINTERGRUND DER ERFINDUNG

[0002] Eine Anmeldung eines Benutzers an einem Endgerät in einem Netzwerk, beispielsweise einem Informationstechnik-System, auch als Computer-Netzwerk bezeichnet, sollte stets gesichert erfolgen, um das Netzwerk vor unberechtigtem Zugriff zu schützen und vertrauliche Daten sicher aufbewahren zu können. Seit längerem wird dabei eine sogenannte Zwei-Faktor-Authentifizierung angewendet. Der sich anmeldende Benutzer muss dazu im Besitz zweier unabhängiger Faktoren sein. Heutzutage weit verbreitet ist die Zwei-Faktor-Authentifizierung mittels einer Chipkarte, auch als Smart Card bezeichnet. Die Verwendung von Smart Cards für eine Zwei-Faktor-Authentifizierung hat einige Nachteile.

[0003] Zunächst muss jede im Netzwerk zu verwendende Smart Card personalisiert werden und an den jeweiligen Benutzer ausgegeben werden. Dies bedarf einer aufwendigen Infrastruktur zur Erstellung der Smart Cards und bedingt zudem ein entsprechendes Ausgabesystem. Der Austausch einer defekten oder einer verloren gegangenen Chipkarte stellt einen erheblichen Mehraufwand dar.

[0004] Jedes Endgerät, an dem sich ein Benutzer authentifizieren muss, benötigt ein entsprechendes Kartenlesegerät. Dieses Lesegerät muss ständig mitgeführt werden, falls das Endgerät im Netzwerk kein entsprechendes Lesegerät aufweist. Das verringert die Benutzerakzeptanz erheblich. Alternativ muss jedes Endgerät mit einem entsprechenden Lesegerät ausgestattet sein, was wiederum die Hardwarekosten für die IT-Infrastruktur erhöht, sofern für das jeweilige Endgerät überhaupt ein Lesegerät verfügbar ist.

[0005] Zudem lassen die Benutzer aus Bequemlichkeit die Smart Card im Lesegerät des Endgeräts stecken und verlassen möglicherweise den Arbeitsplatz ohne die Smart Card mitzunehmen. Dies verringert die Sicherheit im Netzwerk deutlich, da das Endgerät dann durch andere Personen missbräuchlich verwendet werden kann.

[0006] Smart Cards sind bei den Nutzern oft unbeliebt, da sie als zusätzliches Authentifizierungsmittel mitgeführt werden müssen und keinen zusätzlichen Zweck erfüllen, also nach der Authentifizierung am Endgerät nutzlos sind.

[0007] Um diese Einschränkungen zu reduzieren, wird seit einiger Zeit vorgeschlagen, ein Mobiltelefon anstelle einer Smart Card zur Authentifizierung des Benutzers zu verwenden, um eine 2-Faktor-Authentifizierung durchzuführen. Da die meisten Benutzer ein Mobiltelefon besitzen und dieses stets bei sich führen, lassen sich die soeben genannten Nachteile stark reduzieren.

[0008] In der US 7 783 702 B2 wird ein Verfahren zum Zugreifen auf ein Endgerät mittels eines Mobiltelefons via Bluetooth beschrieben. Durch Hinzufügen einer „Engine“ („phone-tocomputer“ bzw. „computer-to-phone“) wird ein Fernzugriff auf das Endgerät durch das mobile Endgerät ermöglicht, wobei dabei ein Authentifizieren am Endgerät durch das mobile Endgerät ermöglicht wird. Als Identität wird die Telefonnummer des mobilen Endgeräts verwendet. Die dabei verwendete Infrastruktur ist nicht abgesichert und ein Angreifer kann sich so leicht Zugriff zum Endgerät verschaffen.

[0009] In der US 2014/0068723 A1 wird eine Zwei-Faktor-Authentifizierung beschrieben. Dieses Verfahren verwendet ein Mobiltelefon, auf dem eine Nachricht angezeigt wird, sobald eine Authentifizierung von einem Authentifizierungsservice, beispielsweise einer Website oder einem Endgerät, angefragt wird. Das Mobiltelefon verwendet zur Identifizierung eine universelle Benutzeridentität, UUID. Hierbei soll das Mobiltelefon das Authentisierungsverhalten des Mobiltelefon-Benutzers erlernen und bei einem erkannten typischen Authentisierungsverhalten, beispielsweise Service und Ort und Zeit, wird das Authentifizieren des Benutzers ohne weitere Benutzerinteraktion ermöglicht. Dieses Verfahren ist hochgradig unsicher, insbesondere wenn ein unberechtigter Dritter das erlernte Muster einfach kopiert und anwendet.

[0010] In der US 8,646,060 B2 wird ein Verfahren zum adaptiven Authentifizieren erläutert. Dabei wird ein Smartphone als Authentifizierungsgerät verwendet, um sich an einem Endgerät anzumelden. Der Benutzer wird automatisch abgemeldet, wenn sich der Benutzer vom Endgerät entfernt. Das Smartphone verwendet dazu beispielsweise eine Bluetooth Verbindung. Dieses Verfahren verwendet einen Kommunikationsserver oder eine Authentifizierungsapplikation. Die Datenübertragung zwischen dem Endgerät und dem Smartphone kann zertifikatsbasiert sein, ei-

ne Public-Key-Infrastruktur, kurz PKI, umfassen und in einem sicheren Speicher oder einem Sicherheitselement ablaufen. Bei Verlust des Mobiltelefons ist eine Zwei-Faktor-Authentifizierung nicht möglich. Der Benutzer kann sich somit nicht sicher an dem System anmelden.

[0011] Somit wird durch die Verwendung von Benutzer-Mobiltelefonen eine einfache Bereitstellung ohne zusätzliche Hardware ermöglicht. Ein entscheidender Nachteil der bisherigen Lösungen zur Authentifizierung mittels eines Mobiltelefons ist das viel geringere Sicherheitsniveau für die Authentifizierung als beispielsweise bei der Verwendung einer Smart Card Lösung. Beispielsweise werden zwar im Mobiltelefon auch kryptografische Schlüssel generiert, diese werden aber durch das Betriebssystem des Mobiltelefons selbst erzeugt, und nur in einem Speicherbereich, beispielsweise einem Software-Container, der direkt vom Betriebssystem aus ansprechbar ist, abgelegt. Ein unberechtigter Dritter kann auf diesem Weg Zugang zu den Schlüsseln erhalten.

[0012] Eine Verbesserung der Sicherheit wird durch das in der US 2015/0121068 A1 beschriebene Verfahren für eine Authentifizierung eines Benutzers an einem Online Service erzielt. Hier wird unter Verwendung einer gesicherten Laufzeitumgebung, englisch Trusted Execution Environment, kurz TEE und einer sicheren Anwendung, englisch Trusted Application, kurz TA, die Sicherheit erhöht. Nur zertifizierte Softwarehersteller haben Zugang zu dieser TEE. Mittels verschiedener Sicherheitsmaßnahmen wird das Verfahren abgesichert, beispielsweise unter Verwendung einer PKI. Eine Authentifizierung an einem Endgerät ist hier allerdings nicht beschrieben.

[0013] Die US 2016/0 330 199 A1 beschreibt ein Verfahren zum Authentifizieren eines Benutzers eines Endgeräts für den Zugriff auf einen Service Provider. Das Authentifizieren wird mittels eines Mobiltelefons des Benutzers durchgeführt. Ist das Mobiltelefon nicht vorhanden, so wird das Authentifizieren mittels eines Mobiltelefons eines Kollegen und einem während der Authentifizierung mittels vom Service.

[0014] Nachteilig bei den bereits existierenden Lösungen ist die fehlende Kompatibilität zu bereits etablierten Systemen. Es fehlt bislang die Möglichkeit eines Mischbetriebs für die Authentifizierung mit Smart Card und Authentifizierung mit einem Mobiltelefon. Zudem muss bei jeder der bisherigen Lösungen zwingend die Smart Card oder das Mobiltelefon vom Benutzer mitgeführt werden. Bei einem Verlust, einem Vergessen, einem Defekt oder einer temporäreren Nichtbetriebsfähigkeit, beispielsweise bei einem zu niedrigen Ladezustand eines Akkumulators, ist in diesen Systemen eine Zwei-Faktor-Authentifizierung nicht mehr möglich. Sofern in der jeweiligen Umgebung erlaubt, wird dann auf eine Ein-Faktor-Lösung zurückgegriffen, die die Sicherheit des Netzwerks deutlich reduziert. Umgebungen, in denen die Nutzung zweier Faktoren obligatorisch ist, erlauben in diesem Fall gar keine Authentifizierung.

[0015] Aufgabe der hier vorliegenden Erfindung ist es, die oben genannten Nachteile zu beseitigen. Insbesondere soll ein Anmeldeverfahren mittels Zwei-Faktor-Authentifizierung bereitgestellt werden, welches einfach und flexibel ist und stets angewendet werden kann.

ZUSAMMENFASSUNG DER ERFINDUNG

[0016] Die Aufgabe wird mit den in den unabhängigen Patentansprüchen beschriebenen technischen Maßnahmen gelöst. Vorteilhafte Ausgestaltungen sind in den jeweils abhängigen Patentansprüchen beschrieben.

[0017] Insbesondere wird die Aufgabe durch ein Verfahren zum Anmelden eines Benutzers an einem Endgerät mittels eines Einmal-Passworts bei Nichtvorhandensein eines zum Authentifizieren des Benutzers zu verwendenden mobilen Endgeräts gelöst. Das Verfahren umfasst dabei die folgenden Schritte: Umschalten des Anmeldevorgangs am Endgerät zum Verwenden eines Einmal-Passworts anstelle einer Authentifizierung mittels des mobilen Endgeräts zum Authentifizieren dieses Benutzers an diesem Endgerät, wobei das Einmal-Passwort bei einer vormaligen Authentifizierung des Benutzers, also einer erfolgreichen Anmeldung des Benutzers am Netzwerk, erzeugt wurde und in einer Registrierungsstelle gespeichert ist; Bereitstellen des Einmal-Passworts an den Benutzer; Abfragen des Einmal-Passworts zum Anmelden mittels einer Berechtigungsanfrage-Routine des Endgeräts; Prüfen des Einmal-Passworts und Authentifizieren des Benutzers an dem Endgerät des Netzwerks; Generieren eines neuen Einmal-Passworts durch die Berechtigungsanfrage-Routine des Endgeräts; und Speichern des neuen Einmal-Passworts in der Registrierungsstelle anstelle des bisherigen Einmal-Passworts und Verwenden des neuen Einmal-Passworts bei einem darauffolgenden Anmelden des Benutzers am Endgeräts bei erneutem Nichtvorhandensein des zum Authentifizieren des Benutzers zu verwendenden mobilen Endgeräts.

[0018] Der Abfragen-Schritt umfasst beispielsweise auch einen Übertragen-Schritt, wobei dabei das eingegebene Einmal-Passwort mittels der Berechtigungsanfrage-Routine des Endgeräts übertragen wird. Besteht während des Authentifizierungsvorgangs keine Verbindung zur Registrierungsstelle wird das Generieren des neuen Einmal-Passworts sowie das Übertragen zur Registrierungsstelle auf einen späteren Zeitpunkt verschoben und dann ausgeführt, wenn eine Kommunikationsverbindung zur Registrie-

rungsstelle vorhanden ist. Bis zu diesem Zeitpunkt behält das ursprüngliche Einmal-Passwort seine Gültigkeit und kann zum Authentifizieren des Benutzers verwendet werden.

[0019] Unter einem Endgerät wird hierbei ein Gerät verstanden, das an einem öffentlichen oder privaten Daten- oder Telekommunikationsnetz angeschlossen ist. Das Endgerät ist beispielsweise ein Client. Ein Client kommuniziert über das Netzwerk mit einem Server, um dessen Dienste abzurufen. Das Endgerät kann ein stationäres Endgerät, also ein Arbeitsplatzrechner, ein PC, eine Workstation oder auch ein tragbares Endgerät, wie ein Notebook, ein Netbook, ein Ultrabook oder ein Tablet-PC sein.

[0020] Ein mobiles Endgerät ist dabei ein Endgerät, das aufgrund seiner Größe und seines Gewichts ohne größere körperliche Anstrengung tragbar und somit mobil einsetzbar ist, beispielsweise ein Endgerät für mobile, netzunabhängige Daten-, Sprach- und Bildkommunikation und Navigation, wie ein Smartphone, ein Mobiltelefon oder ein Handheld.

[0021] Mit Anmelden des Benutzers am Endgerät ist insbesondere dessen Authentifizierung durch das Netzwerk oder das Endgerät gemeint. Dies ist ein Nachweis, also eine Verifizierung, dass der am Endgerät befindliche Benutzer tatsächlich der behauptete Benutzer ist. Der Benutzer authentisiert sich am Netzwerk oder Endgerät und bei Verifizierung des Benutzers gilt der Benutzer als authentisch. Hierbei wird mit dem Anmelden insbesondere der Vorgang einer Berechtigungsprüfung für die Bezeugung ggf. einer Echtheit einer tatsächlich bestehenden Zugangsberechtigung gemeint. Nach einer erfolgreichen Authentifizierung ist der Benutzer im Rahmen seiner Berechtigungen im Netzwerk autorisiert, das Endgerät zu benutzen.

[0022] Das erfindungsgemäße Umschalten des Anmeldevorgangs am Endgerät kann automatisch erfolgen, beispielsweise nach Ablauf einer gewissen Zeitdauer, in der das Endgerät zwar das Vorhandensein eines Benutzers nicht jedoch eines zum Authentifizieren üblicherweise verwendeten mobilen Endgeräts erkannt hat. Das Umschalten kann auch vom Benutzer am Endgerät durch eine Benutzerinteraktion erfolgen. Das Umschalten kann auch mittels eines Fernzugriffs auf das Endgerät über ein Netzwerk erfolgen, beispielsweise auf Basis eines Kommandos einer Registrierungsstelle. Das Umschalten kann das Verändern einer grafischen Benutzeroberfläche, englisch Graphical User Interface, kurz GUI, am Endgerät beinhalten, welche zur Eingabe einer Authentifizierungssequenz auffordert.

[0023] Ein Netzwerk ist dabei ein Rechnernetzwerk oder auch Computemetzwerk, also ein Zusammenschluss verschiedener technischer, primär selbstständiger Endgeräte. Dieser Zusammenschluss ermöglicht die Kommunikation unter den Endgeräten. Ziel ist hierbei die gemeinsame Nutzung von Ressourcen wie Netzwerkdruckern, Servern, Mediendateien und Datenbanken. Wichtig ist auch die Möglichkeit zur zentralen Verwaltung von Endgeräten, Benutzern, deren Berechtigungen und Daten. Für das hier beschriebene Anmeldeverfahren ist das Vorhandensein einer Kommunikationsverbindung zu dem Netzwerk nicht zwingend erforderlich, sodass eine Anmeldung am Endgerät auch in einem sogenannten Offline-Modus des Endgeräts lokal erfolgen könnte.

[0024] Für das erfindungsgemäße Verfahren wird ein Einmal-Passwort verwendet. Ein Einmal-Passwort, englisch One-Time-Password, kurz OTP, ist eine Einmalkennung zur Authentifizierung des Benutzers. Jedes Einmal-Passwort ist in bevorzugter Ausgestaltung nur für eine einmalige Verwendung gültig und kann kein zweites Mal verwendet werden, um den Benutzer zu authentifizieren. Entsprechend erfordert jede Authentifizierung oder Autorisierung ein neues Einmal-Passwort. Es ist sicher gegen passive Angriffe, also einem unberechtigten Mithören. Sogenannte Replay-Attacken sind somit unmöglich. Im Offline-Modus behält das Einmal-Passwort seine Gültigkeit bis das neue Einmal-Passwort erfolgreich mit der Registrierungsstelle ausgehandelt werden konnte.

[0025] Im hier vorgeschlagenen Verfahren wird mit dem OTP die Möglichkeit geschaffen auch ohne das Vorhandensein seines zur Authentifizierung am Netzwerk üblicherweise vorgesehenen mobilen Endgeräts eine Zwei-Faktor-Authentifizierung durchzuführen. Das OTP ist dabei zwingend bei einer vormaligen Authentifizierung des Benutzers generiert worden, das heißt das OTP ist keine von einem System bereitgestellte zufällige Zeichenkette, sondern ein nach erfolgreicher Authentifizierung des Benutzers ausgehandelten Zeichenkette, sodass das OTP das Sicherheitsniveau des sonst verwendeten Benutzerzertifikats des mobilen Endgeräts aufweist. Dieses OTP wird in einer Registrierungsstelle des Netzwerks abgelegt. Für die Verwendung des Einmal-Passworts gibt es zwei Varianten.

[0026] In einer ersten Variante wird das Einmal-Passwort dazu verwendet, ein in einem sicheren Bereich des Endgeräts abgelegtes Ersatz-Benutzerzertifikat zu verschlüsseln. Während der Authentifizierung wird dieses dann mit dem vom Benutzer eingegebenen Einmal-Passwort entschlüsselt und zur Authentifizierung verwendet. Bei falscher Eingabe schlägt der Entschlüsselungsvorgang fehl. In dieser Ausgestaltung wird das Einmal-Passwort nicht auf dem Endgerät gespeichert.

[0027] In einer zweiten Variante wird das Einmal-Passwort mit einem Hash-Algorithmus behandelt (=

gehasht) und auf dem Endgerät gespeichert. Hash-Algorithmen können nicht umgekehrt werden, d.h. aus einem Hashwert lässt sich das ursprüngliche Einmal-Passwort nicht mehr ableiten. Während der Authentifizierung wird das vom Benutzer eingegebene Einmal-Passwort ebenfalls gehasht und mit dem gespeicherten Wert verglichen. In der Folge hat der Benutzer dann die Möglichkeit sich mit Benutzername und Kennwort am Endgerät anzumelden. Das Einmal-Passwort kann durch den Nutzer z.B. telefonisch oder über einen abweichenden Weg von der Registrierungsstelle angefragt werden. Diese hat in diesem Vorgang die Möglichkeit die Identität des Antragsstellers zweifelsfrei zu ermitteln.

[0028] Die Registrierungsstelle ist eine Instanz im Netzwerk und kann beispielsweise als Selbstverwaltungsportal ausgebildet sein, um einem Benutzer die Möglichkeit der selbstständigen Anmeldung an dem erfindungsgemäßen Verfahren zu ermöglichen. Diese Registrierungsstelle erstellt beispielsweise Informationen für eine sichere Anwendung, englisch Trusted Application, kurz TA, in einer gesicherten Laufzeitumgebung, englisch Trusted Execution Environment, kurz TEE, in dem mobilen Endgerät, sodass eine sichere und einfache Initialisierung des erfindungsgemäßen Verfahrens erfolgen kann. Auf Basis des Umschaltens des Anmeldevorgangs prüft die Registrierungsstelle beispielsweise auch, ob der Benutzer für die Nutzung des Endgeräts berechtigt ist. Die Registrierungsstelle kann auch notwendige Konfigurationsdaten übertragen.

[0029] Im Bedarfsfall wird das OTP dem Benutzer bereitgestellt. In einer bevorzugten Ausgestaltung wird das OTP dem Benutzer über eine von der Verbindung zwischen dem Endgerät und dem Netzwerk verschiedene Verbindung bereitgestellt. Dazu führt der Benutzer in einem einfachen Anwendungsfall ein Telefonat oder Video-Telefonat mit beispielsweise einer Service- oder Auskunftsstelle des Netzwerks (Helpdesk) und erbittet das OTP durch mündliche Ansage. Zum Bereitstellen dieses OTP muss sich der Benutzer eindeutig identifizieren, beispielsweise mittels eines Ausweisdokuments oder einem hinterlegten Foto des Benutzers. Die Auskunftsstelle verifiziert anhand der hinterlegten Daten den Benutzer und stellt das OTP bei Übereinstimmung bereit. Alternativ kann das OTP auch über einen anderen Kanal als dem Telefon übertragen werden, beispielsweise einem zweiten mobilen Endgerät des Benutzers oder einem Hardware-Token, beispielsweise USB-Stick oder Speicherkarte. Wichtig ist, dass der Benutzer nur dann das OTP erhält, wenn seine Identität festgestellt wurde, die Identität des Benutzers also zweifelsfrei verifiziert wurde.

[0030] Das OTP wird vom Endgerät abgefragt. Dazu wird eine Berechtigungsanfrage-Routine des Endgeräts, englisch Credential Provider, kurz CP, verwendet. Dieser CP wird zur Authentifizierung des Benutzers insbesondere an einem sogenannten Domain-Controller verwendet, um eine Anmeldung am Endgerät zu ermöglichen. Der CP ist beispielsweise der auf dem Endgerät im Rahmen der erfindungsgemäßen Authentifizierungsanwendung mittels mobilen Endgeräts bereits installierte CP, sodass das Sicherheitsniveau erhalten bleibt. Dieser CP verändert das herkömmliche Anmeldeverfahren an dem Endgerät und ist üblicherweise für eine Kommunikation mit dem mobilen Endgerät verantwortlich. Durch die Nutzung eines CP, der eine Kommunikation mit dem mobilen Endgerät direkt steuert und überwacht, wird das Sicherheitsniveau im System wesentlich erhöht. Der CP ist eine vertrauenswürdige Instanz und ist Teil des Authentifizierungssystems. Der CP verhindert beispielweise, dass ein schädlicher Minitreiber installiert wird, der einem Angreifer ermöglicht, die Kommunikation zwischen dem Endgerät und dem mobilen Endgerät mitzuschneiden. Dieser CP wird nun in vorteilhafter Weise auch bei der Eingabe des OTP verwendet, um zu verhindern, dass das OTP von einem Angreifer abgegriffen wird und zur unberechtigten Anmeldung verwendet wird.

[0031] Der Benutzer verwendet das bereitgestellte OTP sodann in einer entsprechenden Eingabemaske des Endgeräts. Das Endgerät prüft und verifiziert das OTP und ermöglicht so die Authentifizierung des Benutzers. In einer ersten Ausgestaltungsvariante wird das OTP verwendet, um auf ein Ersatz-Zertifikat, welches in einem sicheren Speicherbereich, beispielsweise einem Trusted Platform Module, TPM, des Endgeräts abgelegt ist, zuzugreifen. Diese erste Ausgestaltungsvariante findet Anwendung, wenn eine Anmeldung am Endgerät mittels eines Zertifikats erfolgen muss, beispielsweise auf Grund einer Firmen-Politik zwingend vorgeschrieben ist. Alternativ kann in einer zweiten Ausgestaltungsvariante das OTP als zweiter Faktor zur Anmeldung am Endgerät mit einem Benutzernamen und einem weiteren Passwort genutzt werden. In dieser zweiten Ausgestaltungsvariante wird also eine konventionelle Anmeldung am Endgerät erst nach einer erfolgreichem Prüfung und Verifizierung des OTP freigeschaltet, sodass auch hier die Zwei-Faktor-Authentifizierung erhalten bleibt.

[0032] Sobald die Authentifizierung mit Hilfe des OTP erfolgt ist, wird ein neues OTP durch den CP generiert und in der Registrierungsstelle verschlüsselt abgelegt. Wird das OTP zusammen mit einem Ersatz-Benutzerzertifikat verwendet, so wird dieses ungültig und durch den CP automatisch ein neues angefordert. Dieses neue Zertifikat wird mit dem OTP verschlüsselt und im sicheren Speicher abgelegt. Wird das OTP mit Benutzername und einem weiteren Passwort verwendet, so wird lediglich der Hashwert des alten OTP durch den des neuen ersetzt. Dieses neue OTP ist bei einer erneuten An-

meldung des Benutzers ohne das zum Authentifizieren des Benutzers zu verwendende mobile Endgerät zu verwenden. Besteht zum Zeitpunkt der Authentifizierung keine Verbindung zur Registrierungsstelle wird das Generieren und Übertragen an die Registrierungsstelle auf den Zeitpunkt der Wiederherstellung der Verbindung verschoben.

[0033] Das Übertragen und Ablegen des neuen OTP erfolgt bevorzugt kryptografisch verschlüsselt. Als Verschlüsselung, auch Chiffrierung, wird hierbei die mittels eines Schlüssels erfolgte Umwandlung von Daten im „Klartext“ in Daten im „Geheimtext“, auch: Chiffrat, bezeichnet, sodass der Klartext aus dem Geheimtext nur unter Verwendung eines geheimen Schlüssels wiedergewonnen werden kann. Sie dient zur Geheimhaltung von Nachrichten, beispielsweise um Daten gegenüber unbefugtem Zugriff zu schützen oder um Nachrichten vertraulich übermitteln zu können. Die entsprechenden Schlüssel werden zwischen Endgerät und Registrierungsstelle ausgehandelt oder durch entsprechend sichere Übertragung im Vorfeld verteilt.

[0034] Durch das erfindungsgemäße Verfahren wird eine Zwei-Faktor-Authentisierung stets sichergestellt. Bei der Anmeldung des Benutzers mit seinem mobilen Endgerät ist der erste Faktor der Besitz des mobilen Endgeräts mit dem sich darauf befindlichen Zertifikat. Der zweite Faktor ist eine PIN oder ein biometrischer Wert, beispielsweise ein Fingerabdruck oder ein Augenscan, der zusätzlich vom Benutzer abgefragt wird.

[0035] Bei Verlust, Defekt oder sonstigem Nicht-Vorhandensein des Endgeräts ersetzt das erfindungsgemäße Einmal-Passwort nun den ersten Faktor. Der zweite Faktor wird durch das Telefonat oder Video-Telefonat mit dem Helpdesk und dem dazu erforderlichen Verifizieren der Identität des Benutzers ersetzt. Dabei versichert das Verfahren mit dem Helpdesk, dass es sich bei dem Benutzer tatsächlich um den entsprechenden Mitarbeiter handelt. Das OTP kann dabei endgeräteseitig oder registrierungsstellenseitig erstellt werden. Die Erzeugung des OTP auf dem Endgerät wird sichergestellt, dass dem Endgerät nicht von außen ein manipuliertes und einem Angreifer bekanntes OTP bereitgestellt wird.

[0036] Dieses Verfahren ermöglicht eine sichere Fallback-Methode zum Anmelden an ein Endgerät auch für den Fall, dass das sonst üblicherweise verwendete mobile Endgerät nicht vorhanden ist, beispielsweise aufgrund eines Defekts oder eines Verlusts oder eines niedrigen Akkuladezustands oder bei schlichtem Vergessen dieses. Die Zwei-Faktor-Authentifizierung bleibt erhalten, das Sicherheitsniveau wird dadurch nicht gesenkt und eine einfache Authentifizierung des Benutzers ist ermöglicht. Diese Lösung kann auch angewendet werden, wenn keine Kommunikations-Verbindung zwischen Endgerät und Netzwerk besteht. Somit wird auch eine Offline-Anmeldung ermöglicht. Das neue OTP wird der Registrierungsstelle automatisch zur Verfügung gestellt, sobald eine Kommunikationsverbindung zwischen Endgerät und Netzwerk wieder vorhanden ist.

[0037] Das System stellt somit auch einen Vorteil gegenüber den Smart-Card Lösungen für eine Anmeldung am Endgerät dar, da hier überhaupt keine sichere Möglichkeit geschaffen werden kann, wenn die Smart-Card nicht verfügbar ist. Die erfindungsgemäße Lösung bietet hier die Möglichkeit über ein sicher zwischen dem CP und der Registrierungsstelle ausgehandeltem OTP einen zweiten Faktor für eine einmalige Anmeldung zu nutzen.

[0038] In einer bevorzugten Ausgestaltung wird im Netzwerk ein Verzeichnisdienst zum Authentifizieren des Benutzers verwendet und der Benutzer wird durch erfolgreiche Authentifizierung im Verzeichnisdienst am Endgerät angemeldet. Der Verzeichnisdienst ist vorzugsweise netzwerkweit zentral und im Fall eines Windows™ Betriebssystems das Active Directory, kurz AD. Bei einem solchen Verzeichnis wird ein Netzwerk entsprechend der realen Struktur des Unternehmens oder seiner räumlichen Verteilung gegliedert. Dazu verwaltet es verschiedene Objekte in einem Netzwerk wie beispielsweise Benutzer, Gruppen, Computer, Dienste, Server, Dateifreigaben und andere Geräte wie Drucker und Scanner und deren Eigenschaften. Mit Hilfe von AD können die Informationen der Objekte organisiert, bereitgestellt und überwacht werden. Den Benutzern des Netzwerkes werden entsprechend Zugriffsbeschränkungen erteilt, sodass nicht jeder Benutzer jede Datei oder jedes Netzwerkobjekt einsehen bzw. verwenden kann. Die Anmeldung erfolgt sodann beispielsweise mittels Kerberos-Zertifikats-Authentifizierung. Das OTP kann zusätzlich im Verzeichnisdienst abgelegt werden, um den Zugriff aus existierenden Help-Desk Anwendungen darauf zu erleichtern. Bevorzugt erfolgt die Ablage des OTP verschlüsselt.

[0039] In einer bevorzugten Ausgestaltung wird bei Verlust oder Defekt des mobilen Endgeräts die Gültigkeit des bisherigen Benutzerzertifikats in dem Netzwerk widerrufen. Ein (digitales) Zertifikat, ist dabei ein digitaler Datensatz, der bestimmte Eigenschaften des Benutzers bestätigt und dessen Authentizität und Integrität durch kryptografische Verfahren geprüft werden kann. Das digitale Zertifikat enthält insbesondere die zu seiner Prüfung erforderlichen Daten. Insbesondere sind für diese Erfindung die Public-Key-Zertifikate der Public-Key-Infrastruktur, kurz PKI, relevant, die beispielsweise nach dem Standard X.509 definiert sind und welche die Identität des Inhabers und weitere Eigenschaften eines öffentlichen kryptografischen Schlüssels bestätigen.

[0040] Public-Key-Zertifikate enthalten in der Regel den Namen (oder eine andere eindeutige Bezeichnung) der zuvor erwähnten Zertifizierungsstelle; Informationen zu den Regeln und Verfahren, unter denen das Zertifikat ausgegeben wurde; Informationen zur Gültigkeitsdauer des Zertifikates; den öffentlichen Schlüssel, zu dem das Zertifikat Angaben macht; den Namen (oder eine andere eindeutige Bezeichnung) des Eigentümers (= Benutzers) des öffentlichen Schlüssels; weitere Informationen zum Eigentümer des öffentlichen Schlüssels; Angaben zum zulässigen Anwendungs- und Geltungsbereich des öffentlichen Schlüssels und eine digitale Signatur des Ausstellers über alle anderen Informationen.

[0041] Die Gültigkeit des digitalen Zertifikates ist meist auf einen im Zertifikat festgelegten Zeitraum begrenzt. In dem vorliegenden Verfahren kann die Gültigkeit eines Zertifikats widerrufen werden, wenn bei Nichtvorhandensein des mobilen Endgeräts dennoch eine Authentifizierung des Benutzers im Netzwerk zum Anmelden an ein Endgerät erfolgen soll. Dies erfolgt bevorzugt dann, wenn das mobile Endgerät durch Verlust oder technischen Defekt absehbar nicht mehr verwendet wird. Damit wird sichergestellt, dass das Benutzerzertifikat nicht von einem Angreifer zum Anmelden am Netzwerk verwendet wird. In minderschweren Fällen, wie der Nichtbenutzbarkeit durch einen leeren Akkumulator bleibt die Gültigkeit des Zertifikats bestehen.

[0042] In einer bevorzugten Ausgestaltung wird die Berechtigungsanforderungs-Routine jedes neue Einmal-Passwort mit der Registrierungsstelle aushandeln und das neue Einmal-Passwort kryptografisch gesichert, beispielsweise mittels asymmetrischer oder symmetrischer Verschlüsselung, übertragen. Auf diese Weise ist ein Angreifer nicht in der Lage die Fallback-Methode zu korrumpieren.

[0043] Das OTP wurde dazu zwischen einer sicheren Laufzeitumgebung des mobilen Endgeräts und einer Instanz des Netzwerks, beispielsweise der Registrierungsstelle ausgehandelt. Dazu wird ein kryptografisches Challenge-Verfahren, beispielsweise gemäß dem Challenge Handshake Authentication Protocol, kurz CHAP, angewendet. Nachfolgend wird der Begriff OTP-Generieren mit OTP-Aushandeln gleichgesetzt.

[0044] In einer bevorzugten Ausgestaltung wird zum Authentifizieren des Benutzers ein neues Benutzerzertifikat erstellt, wobei dieses Erstellen die folgenden Verfahrensschritte umfasst: Einrichten (Installieren) einer sicheren Anwendung auf einem weiteren mobilen Endgerät; Verbinden der sicheren Anwendung zu einem Verwaltungssystem zum Aktivieren der sicheren Anwendung; Erstellen von neuen Schlüsseln zur Verwendung in kryptographischen Verfahren in der sicheren Anwendung; Anfragen und Erhalten des neuen Benutzerzertifikats bei einer Zertifizierungsstelle durch die aktivierte sichere Anwendung; Anmelden des Benutzers unter Verwendung des neuen Benutzerzertifikats der sicheren Anwendung und der Berechtigungsanfrage-Routine des Endgeräts im Netzwerk; Generieren eines neuen Einmal-Passworts durch die Berechtigungsanfrage-Routine des Endgeräts; Speichern des neuen Einmal-Passworts in der Registrierungsstelle anstelle des bisherigen Einmal-Passworts und Verwenden des neuen Einmal-Passworts bei einem darauffolgenden Anmelden des Benutzers am Endgeräts bei erneutem Nichtvorhandensein des zum Authentifizieren des Benutzers zu verwendenden mobilen Endgeräts.

[0045] Die sichere Anwendung TA läuft dabei bevorzugt in der sicheren Laufzeitumgebung TEE des mobilen Endgeräts ab. Das Benutzerzertifikat wird für ein kryptografisches Schlüsselpaar generiert, welches in einem nur für die sichere Laufzeitumgebung zugreifbaren sicheren Speicherbereich des mobilen Endgeräts abgelegt ist.

[0046] Die TA wird auf dem mobilen Endgerät des Benutzers installiert. Diese TA wird in der Benutzerzertifikat-Erstellungsphase eingesetzt, um das Schlüsselpaar, das die Basis des Benutzerzertifikats bildet, zu erzeugen. Außerdem wird diese TA im üblichen Anmeldeverfahren verwendet, um sämtliche kryptographischen Operationen während der Authentifizierung des Benutzers auszuführen. Hierzu wird das Endgerät ausgewählt und die TA gestartet. Innerhalb des üblichen Anmeldeverfahrens muss der Benutzer stets beweisen, dass er für dieses Schlüsselpaar zugriffsberechtigt ist. Dies kann er über eine PIN oder einen der biometrischen Sensoren des neuen mobilen Endgeräts tun. Zusammen mit der TA wird in bevorzugter Ausgestaltung auch ein Service auf dem mobilen Endgerät installiert. Dieser Service prüft das Sicherheitsniveau des neuen mobilen Endgeräts automatisch. So erkennt das Anmeldeverfahren automatisch, ob das neue mobile Endgerät sicher ist oder gerooted wurde und ob alle relevanten Sicherheits-Patches eingespielt wurden. Ist dies nicht der Fall, kann dieses neue mobile Endgerät nicht als zweiter sicherer Faktor verwendet werden. Die TA ist beispielsweise eine Anwendung für die Betriebssysteme Android™ oder iOS™ und ermöglicht neben der normalen Programmbearbeitung die Ausführung von Programmcode innerhalb einer TEE auf dem mobilen Endgerät oder einem alternativ geschützten Bereich im mobilen Endgerät und wird daher als sichere Anwendung bezeichnet. Der in der TEE ablaufende Teil der TA generiert und speichert das Schlüsselpaar im neuen mobilen Endgerät.

[0047] Das Verwaltungssystem für sichere Anwendungen, englisch Trusted Application Manager, kurz TAM, ist eine Instanz des Netzwerks oder eines entfernten Systems und prüft eine Lizenz und auch eine

Registrierung der sicheren Anwendung. Dieser TAM, auch Trusted Server, ist für den Aufbau eines sicheren Kanals in das TEE des neuen mobilen Endgeräts verantwortlich. Dieser Kanal kann nicht vom Betriebssystem des mobilen Endgerätes eingesehen werden.

[0048] In einer bevorzugten Ausgestaltung werden für den oben genannten Verbinden-Schritt Informationen von der Registrierungsstelle zum Erzeugen einer Verbindung zum TAM in der TA erhalten. Diese Informationen können beispielsweise als QR-Code bereitgestellt und mittels einer Kamera des mobilen Endgeräts erfasst werden.

[0049] In einer bevorzugten Ausgestaltung beinhalten die Informationen von der Registrierungsstelle zudem Informationen für das Abrufen des Benutzerzertifikats von der Zertifizierungsstelle, beispielsweise auf Basis des Simple Certificate Enrollment Protocolls, kurz SCEP. Die Datenübertragung von der Registrierungsstelle erfolgt beispielsweise mittels QR-Code. Aufgrund der rein optischen Natur dieses Übertragungswegs ist ein Abhören des Funkfrequenzraums für einen Angriff nutzlos.

[0050] Der erfindungsgemäße Anmeldeschritt bei Authentifizieren mittels mobilem Endgerät umfasst bevorzugt die Schritte: Starten der sicheren Anwendung auf dem mobilen Endgerät und Aufbauen einer drahtlosen Kommunikationsverbindung vom mobilen Endgerät zu dem Endgerät; Starten der Berechtigungsanfrage-Routine im Endgerät und Aufbau einer Kommunikationsverbindung zum Netzwerk zur Authentifizierung des Benutzers; Generieren einer Berechtigungsaufforderung durch das Netzwerk und Übertragen dieser an das Endgerät; Freischaltung des Benutzerzertifikats im mobilen Endgerät durch Eingabe einer PIN oder durch Nutzung eines biometrischen Sensors; Signieren der Berechtigungsaufforderung mittels des Benutzerzertifikats in der sicheren Anwendung; Übertragen der signierten Berechtigungsaufforderung an das Netzwerk zum Prüfen der Signatur und der Gültigkeit des Zertifikats; und Erteilen einer Anmelde-Erlaubnis vom Netzwerk bei erfolgreicher Prüfung.

[0051] Dieses Anmeldeverfahren umgeht die Nachteile einer Smart Card Anmeldung und einer unsicheren Anmeldung mittels mobilem Endgerät gleichermaßen. Diese Lösung kann vom Benutzer selbst in Betrieb genommen werden, bei Austausch oder bei Verlust des mobilen Endgeräts kann eine Anmeldung trotzdem erfolgen. Das mobile Endgerät ist ein eigenständiges Endgerät und wird meist getrennt vom Endgerät auf dem sich der Benutzer anmelden möchte, transportiert, sodass auch die Benutzerakzeptanz für das erfindungsgemäße Verfahren steigt.

[0052] Mit diesem Anmeldeverfahren werden die benötigten Schlüssel direkt auf dem mobilen Endgerät innerhalb einer TEE erzeugt. Dies ist vom Sicherheitsniveau vergleichbar mit der Schlüsselerzeugung innerhalb eines Krypto-Prozessors einer Smart Card. Bevorzugt wird ein kryptografisches Verschlüsselungsverfahren angewendet, insbesondere ein asymmetrisches Verschlüsselungsverfahren. Der private Schlüssel des generierten Schlüsselpaars verlässt das mobile Endgerät nicht. Nur über die TEE kann darauf zugegriffen werden. Sämtliche Operationen bezüglich dieses Schlüsselpaars finden ebenfalls innerhalb des TEE statt.

[0053] Das Endgerät erhält den CP. Dieser CP stellt die Kommunikation mit dem mobilen Endgerät vollständig transparent für das Betriebssystem zur Verfügung. Die Kommunikation zwischen Endgerät und mobilen Endgerät ist funkbasiert, beispielsweise mittels Nahbereichs-Technik nach dem Standard Bluetooth LE, die sicherstellt, dass der Benutzer des mobilen Endgeräts auch physisch in der Nähe des Endgeräts ist. Ein Mischbetrieb ist jederzeit möglich, so dass der Benutzer auch andere Authentifizierung nutzen kann. Über eine Auswertung der Feldstärkemessung kann erkannt werden, ob ein Benutzer sich einem Endgerät nähert oder von diesem entfernt und dementsprechend kann der CP eine Anmeldeprozedur einleiten oder den Benutzer abmelden.

[0054] Bevorzugt erkennt das Endgerät bei der Anmeldung automatisch die Verfügbarkeit eines gekoppelten mobilen Endgeräts und meldet den Benutzer an, wenn dieser die TA gestartet hat und sich mit der PIN oder einem geeigneten biometrischen Sensor an dieser angemeldet hat. Der Benutzer muss am Endgerät keine Auswahl des CP treffen, sondern lediglich in Kommunikationsreichweite des Endgerätes sein.

[0055] Im Gegensatz zu anderen Lösungen, die mobile Endgeräte einsetzen, funktioniert dieses Verfahren auch, wenn das mobile Endgerät und/oder das Endgerät keine Verbindung zum Netzwerk hat. Dies wird durch die direkte Kommunikation zwischen mobilen Endgerät und dem Endgerät auf dem sich der Benutzer anmelden möchte, erreicht. Auf die Nutzung eines zentralen Anmeldeservers wird verzichtet.

[0056] Im Erfindungsgedanken ebenfalls enthalten ist ein mobiles Endgerät zum Anmelden eines Benutzers an ein Endgerät eines Netzwerks gemäß dem vorhergehend beschriebenen Verfahren. Das mobile Endgerät umfasst eine gesicherte Laufzeitumgebung beinhaltend die sichere Anwendung; ein Drahtlosverbindungsmodul, beispielsweise Bluetooth LE Modul, eingerichtet zur Kommunikation mit einer Berechtigungsanfrage-Routine eines Endgeräts; einem weiteren Drahtlosverbindungsmodul, insbesondere Mobilfunk- oder Breitbandverbindungsmodul, eingerichtet zur Kommunikation mit einer Zertifizierungsstelle zum Erhalten eines Benutzerzertifikats; einem Spei-

cherbereich zum gesicherten Ablegen eines Schlüsselpaars, wobei die gesicherte Laufzeitumgebung eingerichtet ist, exklusiv auf den Speicherbereich zuzugreifen; und einer Kamera zum Erfassen von Informationen einer Registrierungsstelle.

[0057] Im Erfindungsgedanken ist ebenfalls ein Computerprogrammprodukt enthalten, welches ausführbar in einer sicheren Laufzeitumgebung eines mobilen Endgeräts eingebracht ist und welches zum Authentifizieren eines Benutzers an einem Netzwerk eingerichtet ist, wobei dazu das vorhergehend beschriebene Verfahren durchgeführt wird. Dieses Computerprogrammprodukt beinhaltet insbesondere die sichere Anwendung im mobilen Endgerät.

[0058] Im Erfindungsgedanken ist zudem auch ein Computerprogrammprodukt enthalten, welches ausführbar in einem Endgerät eines Netzwerks eingebracht ist und welches zum Abfragen einer Berechtigung eines Benutzers eingerichtet ist, wobei dazu das vorhergehend beschriebene Verfahren durchgeführt wird. Dieses Computerprogrammprodukt ist insbesondere die Berechtigungsanfrage-Routine im Endgerät.

Figurenliste

[0059] Nachfolgend wird anhand von Figuren die Erfindung bzw. weitere Ausführungsformen und Vorteile der Erfindung näher erläutert, wobei die Figuren lediglich Ausführungsbeispiele der Erfindung beschreiben. Gleiche Bestandteile in den Figuren werden mit gleichen Bezugszeichen versehen. Die Figuren sind nicht als maßstabsgetreu anzusehen, es können einzelne Elemente der Figuren übertrieben groß bzw. übertrieben vereinfacht dargestellt sein.

[0060] Es zeigen:

Fig. 1 ein Ausführungsbeispiel eines Verfahrensablaufdiagramms eines erfindungsgemäßen Verfahrens;

Fig. 2 ein erstes Ausführungsbeispiel eines erfindungsgemäßen Systems zum Authentifizieren eines Benutzers an einem Endgerät;

Fig. 3 ein zweites Ausführungsbeispiel eines erfindungsgemäßen Systems zum Authentifizieren eines Benutzers an einem Endgerät;

Fig. 4 ein Ausführungsbeispiel eines Verfahrensablaufs zum erfindungsgemäßen Einrichten der Authentifizierung eines Benutzers mittels mobilem Endgerät; und

Fig. 5 ein Ausführungsbeispiel eines Verfahrensablaufs zum erfindungsgemäßen Anmelden eines Benutzers an einem Endgerät mittels mobilem Endgerät.

Fig. 6 ein erstes Ausführungsbeispiel eines Verfahrensablaufs zum erfindungsgemäßen Anmelden eines Benutzers an einem Endgerät ohne mobiles Endgerät.

Fig. 7 ein zweites Ausführungsbeispiel eines Verfahrensablaufs zum erfindungsgemäßen Anmelden eines Benutzers an einem Endgerät ohne mobiles Endgerät.

FIGURENBESCHREIBUNG

[0061] In **Fig. 1** ist ein Ausführungsbeispiel eines Verfahrensablaufdiagramms für das erfindungsgemäße Verfahren **100** dargestellt. Das Verfahren **100** ist zum Anmelden eines Benutzers an einem Endgerät mittels eines Einmal-Passworts bei Nichtvorhandensein eines zum Authentifizieren des Benutzers üblicherweise zu verwendenden mobilen Endgeräts vorgesehen. Das Verfahren **100** umfasst einen Umschalten-Schritt **101** zum Umschalten des Anmeldevorgangs am Endgerät zum Verwenden des Einmal-Passworts (OTP) anstelle einer Authentifizierung mittels des mobilen Endgeräts zum Authentifizieren dieses Benutzers an diesem Endgerät. Das Einmal-Passwort wurde bei einer vormaligen Authentifizierung des Benutzers im Endgerät erzeugt und hinterlegt sowie in einer Registrierungsstelle gespeichert. Das Verfahren **100** umfasst zudem einen Bereitstellen-Schritt **102** zum Bereitstellen des Einmal-Passworts an den Benutzer. Das Verfahren **100** umfasst zudem einen Abfragen-Schritt **103** zum Abfragen des Einmal-Passworts zum Anmelden mittels einer Berechtigungsanfrage-Routine des Endgeräts und ggf. Übertragen des eingegebenen Einmal-Passworts mittels der Berechtigungsanfrage-Routine des Endgeräts. Das Verfahren **100** umfasst auch einen Prüfen-Schritt **104** zum Prüfen des Einmal-Passworts mittels einer Berechtigungsanfrage-Routine des Endgeräts und Authentifizieren des Benutzers an dem Endgerät. Das Verfahren **100** umfasst auch einen Generieren-Schritt **105** zum Generieren eines neuen Einmal-Passworts durch die Berechtigungsanfrage-Routine des Endgeräts und das Hinterlegen in diesem. Das Verfahren **100** umfasst schließlich auch einen Speichern-Schritt **106** zum Speichern des neuen Einmal-Passworts in der Registrierungsstelle anstelle des bisherigen Einmal-Passworts und Verwenden des neuen Einmal-Passworts bei einem darauffolgenden Anmelden des Benutzers am Endgeräts bei erneutem Nichtvorhandensein des zum Authentifizieren des Benutzers zu verwendenden mobilen Endgeräts.

[0062] Dieses Verfahren **100** wird im Rahmen der Beschreibung des Systems gemäß der **Fig. 2** und **Fig. 3** sowie der Verfahrensablaufdiagramme gemäß der **Fig. 4** und **Fig. 5** näher erläutert. Das System zur Umsetzung des Authentifizierungsverfahrens mit einem mobilen Endgerät bedingt eine Zertifizierungsstelle mit einer Schnittstelle zum Erstellen ei-

nes Benutzerzertifikats auf Basis eines generierten Schlüsselpaars, ein mobiles Endgerät mit Bluetooth-Drahtloskommunikation, einem Endgerät mit Bluetooth-Drahtloskommunikation, eine sichere Anwendung in einer TEE des mobilen Endgeräts zum Erzeugen, Verwalten und Benutzen von einem kryptografischem Schlüsselpaar (öffentlicher und privater Schlüssel) und eine Berechtigungsanfrage-Routine auf dem Endgerät zum Kommunizieren mit der TA.

[0063] In der **Fig. 2** ist ein erstes Ausführungsbeispiel eines erfindungsgemäßen Systems zum Authentifizieren eines Benutzers an einem Endgerät **1** dargestellt. Das System besteht aus dem Endgerät **1**, welches eine Berechtigungsanfrage-Routine **9**, nachfolgend als Credential Provider CP **9** bezeichnet, beinhaltet. Das System besteht zudem aus einem mobilen Endgerät **2**, welches zum Authentifizieren eines Benutzers (nicht dargestellt) am Endgerät **1** verwendet wird. Das mobile Endgerät **2** umfasst eine sichere Laufzeitumgebung, auch als TEE bezeichnet (nicht dargestellt) und eine sichere Anwendung **8**, auch als TA **8** bezeichnet. Die TA **8** ist eingerichtet, um auf einen sicheren Speicherbereich des mobilen Endgeräts **2** zuzugreifen, in welchem ein von dem mobilen Endgerät **2** generiertes Schlüsselpaar **11** abgelegt ist. Das mobile Endgerät **2** umfasst weiterhin ein Drahtloskommunikationsmodul, um mit dem Endgerät **1** eine Bluetooth-LE-Kommunikation **6** aufzubauen und darüber Daten zum Anmelden und Authentifizieren des Benutzers auszutauschen.

[0064] Bluetooth LE, kurz BLE, ist eine Funktechnik, mit der sich die beiden Endgeräte **1** und **2** in einer Umgebung von etwa 10 Metern vernetzen können, wobei dazu ein vergleichsweise geringer Stromverbrauch benötigt wird. Ein Vorteil von BLE ist, dass die Feldstärke zwischen den verbundenen Endgeräten **1** und **2** ausgewertet werden kann und man so die ungefähre Entfernung angeben kann, ab der die Verbindung als unzureichend gewertet und das Endgerät **1** gesperrt wird. Auf Grund des CP **9** und der TA **8** wird es trotz der limitierten Verbindungsparameter in BLE ermöglicht, eine Zertifikatsanmeldung durchzuführen.

[0065] Das System umfasst zudem eine Registrierungsstelle **3**, auf der eine Registrierungsanwendung **10** eingerichtet ist. Das Endgerät **1** und die Registrierungsstelle **3** sind beispielsweise Objekte des gleichen Netzwerks **13**. Die Kommunikation zwischen dem Endgerät **1** und der Registrierungsstelle **3** erfolgt beispielsweise über eine drahtgebundene Verbindung, wie LAN, oder drahtlos über WLAN oder eine Breitband-Mobilfunkverbindung, wie LTE. Die Registrierungsstelle **3** ist beispielsweise als Selbstverwaltungs-Portal aufgebaut, um einem Benutzer das Einrichten des Anmeldeverfahrens zu ermöglichen. Hier können Informationen für eine Installation der TA **8** und des CP **9** abgerufen werden, sollte das Netzwerk **13** diese Informationen nicht anderweitig zur Verfügung stellen. In der Registrierungsstelle **3** wird die Berechtigung des Benutzers dahingehend geprüft, ob er überhaupt für die Nutzung des Endgeräts **1** freigegeben ist. Die Registrierungsstelle **3** überträgt die notwendigen Konfigurationsdaten einschließlich eines für das Generieren eines dazugehörigen Benutzerzertifikats benötigten SCEP-OTP der Zertifizierungsstelle mittels eines QR-Codes an das mobile Endgerät **2**. Das mobile Endgerät **2** weist eine Kamera (nicht dargestellt) auf, um den QR-Code zu erfassen. Der QR-Code wird sodann mittels eines Prozessors des mobilen Endgeräts **2** ausgewertet und so die Informationen des QR-Codes erhalten. Die Informationen des QR-Codes stellen beispielsweise die Verbindungsinformationen zum TAM **5** bereit. Diese Informationen stellen zudem die Informationen zum Verbindungsaufbau und zum Anfragen des Benutzerzertifikats in einer Zertifizierungsstelle **4** auf Basis eines Schlüsselpaars **11**, beispielsweise ein SCEP-OTP, dar. Durch die Verwendung von QR-Codes und der damit verbundenen optischen Informationsübertragung an das mobile Endgerät **2** ist ein Mitschneiden der Funk-Kommunikation **6** wirkungslos.

[0066] Alternativ können die Informationen der Registrierungsstelle **3** auch über das Netzwerk **13** an das Endgerät **1** übertragen werden und von dort an das mobile Endgerät **2** übertragen werden. Weiterhin alternativ können die Informationen der Regierungsstelle **3** auch über ein Mobilfunknetz (nicht dargestellt) oder ein alternatives Breitbandnetz, bspw. WLAN, direkt an das mobile Endgerät **2** übertragen werden. Alternativ können auch nur erste Teile der Informationen der Registrierungsstelle **3** über den QR-Code empfangen werden, wobei weitere Teile der Informationen der Regierungsstelle **3** über das Mobilfunknetz/Breitbandnetz oder das Netzwerk **13** an das mobile Endgerät **2** übertragen werden.

[0067] Das System umfasst zudem eine Zertifizierungsstelle **4**, englisch Certificate Authority, kurz CA **4**, also eine Instanz, die digitale Zertifikate, so auch das Benutzerzertifikat **14**, herausgibt. Ein digitales Zertifikat dient dazu, den rechtmäßigen Besitz eines Schlüssels nachzuweisen und so zu garantieren, dass die im Zertifikat genannte Identität authentisch ist. Diese Zuordnung wird von der Zertifizierungsstelle **4** beglaubigt, indem sie sie mit ihrer eigenen digitalen Unterschrift (=Signatur) versieht.

[0068] Die im erfindungsgemäßen System verwendeten digitalen Zertifikate **14** enthalten kryptografische Schlüssel und Zusatzinformationen, die zur Authentifizierung des Benutzers und auch zur Verschlüsselung und Entschlüsselung vertraulicher Daten dienen, die sodann über das Netzwerk **13** oder auch das Mobilfunknetz oder alternative Breitbandnetze verbreitet werden. Als Zusatzinformationen

sind zum Beispiel Gültigkeitsdauer, Verweise auf Zertifikatsperrlisten etc. enthalten, die durch die CA **4** mit in das Zertifikat **14** eingebracht werden. Die Aufgabe der CA **4** ist es, diese digitalen Benutzerzertifikate **14** herauszugeben und zu überprüfen. Sie trägt dabei die Verantwortung für die Bereitstellung, Zuweisung und Integritätssicherung der von ihr ausgegebenen Zertifikate. Damit bildet sie den Kern der Public-Key-Infrastruktur, kurz PKI.

[0069] Die CA **4** ist nicht zwangsläufig Teil des Netzwerks **13** und kann eine externe Instanz sein. Die CA **4** stellt das Benutzerzertifikat **14** für das im mobilen Endgerät **2** generierte Schlüsselpaar **11** aus. Dabei verlässt der vertrauliche Schlüssel, auch privater Schlüssel genannt, nicht das TEE des mobilen Endgeräts **2**. Die CA **4** erstellt das Zertifikat **14** und gibt dieses an das mobile Endgerät **2** zurück. Für die Verteilung wird das SCEP verwendet.

[0070] Das System umfasst zudem ein Verwaltungssystem **5**, englisch Trusted Application Manager, kurz TAM **5**. Dieser TAM **5** ist für den Aufbau eines sicheren Kanals in das TEE des mobilen Endgeräts **2** verantwortlich. So können Daten an das mobile Endgerät **2** übertragen werden, ohne dass diese vom Betriebssystem des mobilen Endgeräts **2** abgehört werden können.

[0071] Der TAM **5** registriert die TA **8** und prüft die Lizenz der TA **8** mittels einer damit verbundenen Lizenzvergabestelle **7**. Der TAM **5** ist ebenfalls dazu in der Lage, das im mobilen Endgerät **2** zu verwendende Schlüsselpaar **11** zu generieren und in der TA abzulegen, sollte die TA **8** dazu nicht eingerichtet sein, beispielsweise bei Verwendung von RSA Schlüsseln anstelle von bislang in TEE generierbaren Elliptische-Kurven-Kryptografie-, kurz ECC-, Schlüsseln. Die Kommunikation zwischen TA **8** und TAM **5** ist kryptografisch gesichert.

[0072] Das System gemäß **Fig. 2** umfasst demnach eine PKI, bestehend aus generierten Schlüsselpaaren **11** und mittels Zertifizierungsstelle **4** erzeugten Benutzerzertifikaten **14**. Eine Registrierungsstelle **3** stellt die zur Initialisierung von TA **8** und CP **9** benötigten Informationen bereit. Dazu wird eine Registrierungsanwendung **10** verwendet. Die TA **8** ist in einem TEE des mobilen Endgeräts **2** welche mittels TAM **5** und Lizenzvergabestelle **7** konfigurierbar ist. Die Kommunikation **6** zwischen Endgerät **1** und mobilem Endgerät **2** ist BLE-basiert.

[0073] In **Fig. 3** ist ein zweites Ausführungsbeispiel eines erfindungsgemäßen Systems zum Authentifizieren eines Benutzers an einem Endgerät **1** gezeigt. Das System gemäß **Fig. 3** entspricht in Gänze dem System gemäß **Fig. 2** und es wird nachfolgend lediglich auf die Unterschiede zwischen diesen Systemen hingewiesen.

[0074] In **Fig. 3** sind weitere Server-Dienste **15** dargestellt, die für das Protokollieren der aufgetretenen Ereignisse sowie für die Kommunikation mit Dritt-Systemen verwendet werden können. So können beispielsweise die erstellten Zertifikate **14** in ein Card-Management-System, kurz CMS, übertragen werden, so dass die Anmeldeberechtigung auch direkt vom Netzwerk **13** entzogen werden kann. Als weitere Option kann bei einer online Anmeldung über die TA **8** und/oder das CP **9** ein OTP generiert und sicher verschlüsselt in der TA **8** und dem Server **15** gespeichert werden. Sollte der Benutzer offline sein und keinen Zugriff auf das mobile Endgerät **2** haben, kann über das erfindungsgemäße System, beispielsweise mittels einer Auskunftsstelle (Help-Desk) oder die Registrierungsstelle **3** das OTP - nach hinreichender Identifizierung des Benutzers - erfragt werden, um sich anzumelden.

[0075] Zusätzlich zu dem in **Fig. 2** gezeigten System wird hierbei die Historie über das Schlüsselpaar **11** des Benutzers in der TA **8** abgespeichert. Diese Historie wird von der Registrierungsstelle **3**, dem weiteren Server **15** oder der Zertifizierungsstelle **4** abgefragt. Diese Kommunikation ist basierend auf einem Public-Key Cryptography Standard, kurz PKCS, also einem Standard für asymmetrische Kryptographie, beispielsweise einer PKCS#11 Schnittstelle oder einem Minitreiber oder einem CMP-Protokoll, welches der weitere Server **15** unterstützen sollte. Da sodann private Schlüssel der TA **8** zu transportieren sind, sind verschiedene Szenarien **a**) bis c) dafür denkbar:

a) Die Registrierungsstelle **3** erhält die Schlüsselhistorie von dem weiteren Server **15** als PKCS#12 Datei und verschlüsselt dieses mit dem öffentlichen Schlüssel des Benutzerzertifikats **14**. Die TA **8** verbindet sich mit der Registrierungsstelle **3** in einer TLS-Sitzung. Die TA **8** lädt die verschlüsselte PKCS#12 Datei herunter, entschlüsselt diese Datei mit dem privaten Schlüssel des Schlüsselpaars **11** und speichert die Datei im TEE des mobilen Endgeräts **2**.

b) Die Registrierungsstelle **3** erhält die Schlüsselhistorie von dem weiteren Server **15** als PKCS#12 Datei und sendet diese als PUSH-Nachricht zum Endgerät **1** in verschlüsselter Form. wobei dazu der kryptografische Schlüssel während der Initialisierungsphase der TA **8** verwendet wird.

c) Die Registrierungsstelle **3** erhält die Schlüsselhistorie von dem weiteren Server **15** als PKCS#12 Datei und teilt diese Datei in verschiedene Teile, um als QR-Code an das mobile Endgerät **2** übertragen zu werden. Die Erfassung des QR-Codes mittels Kamera des mobilen Endgeräts **2** erfolgt gleichermaßen, wie in der Initialisierungsphase des Systems zum Bereitstellen der Informationen der Registrierungsstelle **3**. Wichtig ist hierbei, dass die Informationen verschlüs-

selt werden mit dem öffentlichen Schlüssel des Benutzerzertifikats **11** und erst danach in einen QR-Code gewandelt werden. Die Kamera des mobilen Endgeräts **2** erfasst die Informationen des QR-Codes und entschlüsselt die Informationen mit dem privaten Schlüssel des Schlüsselpaars **11** zur Speicherung in der TEE.

[0076] In **Fig. 4** wird ein Ausführungsbeispiel eines Verfahrensablaufs zum erfindungsgemäßen Einrichten der Authentifizierung eines Benutzers zum Anmelden des Benutzers an einem Endgerät **1** mittels seinem mobilem Endgerät **2** gezeigt.

[0077] Das Verfahren gemäß **Fig. 4** weist das Endgerät **1**, das mobile Endgerät **2**, die Registrierungsstelle **3**, die Zertifizierungsstelle **4** (CA **4**) und das Verwaltungssystem **5** (TAM **5**) gemäß den zuvor beschriebenen **Fig. 2** und **Fig. 3** auf.

[0078] In einem Schritt a wird der Benutzer in der Registrierungsstelle **3** für das System freigeschaltet. Die Identität des Benutzers kann dabei aus dem Verzeichnisdienst **12** übernommen werden. Die Registrierungsstelle **3** verbindet sich im Schritt **a'** zudem mit der CA **4**, um für das Beantragen des Benutzerzertifikats benötigten Informationen abzurufen. Zusätzlich veranlasst die Registrierungsstelle **3** die Installation des CP **9** im Endgerät **1** gemäß Schritt **b**, beispielsweise über das Netzwerk **13**, sofern dieser über andere Methoden nicht bereits auf dem Endgerät installiert wurde. Zusätzlich wird im Schritt **c** die TA **8** auf dem mobilen Endgerät **2** installiert.

[0079] Die CA **4** überträgt in Schritt **a'** ein SCEP-OTP für die Erstellung des Benutzerzertifikats **14** zurück an die Registrierungsstelle **3**. Alternativ kann das SCEP-OTP auch direkt von der CA **4** an das mobile Endgerät **2** übertragen werden. Die Schritte **a**, **b** und **c** können zeitgleich oder hintereinander ausgeführt werden.

[0080] Die Registrierungsstelle **3** erstellt im Schritt **d** einen QR-Code. Dieser QR-Code beinhaltet Informationen für das mobile Endgerät **2**. Die Informationen können ein Bündel an Informationen darstellen, beinhaltend das SCEP-OTP von der CA **4**, Verbindungsinformationen zur CA **4** und Verbindungsinformationen zum TAM **5**. Diese Informationen können ggf. auch in getrennte QR-Codes gewandelt und dem mobilen Endgerät **2** bereitgestellt werden.

[0081] Der QR-Code oder die QR-Codes werden im Schritt **e** von dem mobilen Endgerät **2** durch Erfassen des QR-Codes mittels Kamera empfangen. Alternativ können die im QR-Code enthaltenen Informationen auch über andere Wege wie z.B. das Netzwerk **13** oder in anderen Formaten übertragen werden. Sodann wird die TA **8** eingerichtet, wobei der QR-Code ausgelesen wird, um die TA **8** einzurichten.

[0082] Während des Einrichten-Schritt e verbindet sich die TA **8** auf Basis der im QR-Code enthaltenen Verbindungsinformationen mit dem TAM **5** im Schritt **f**. Im TAM **5** wird die Lizenz der TA **8** geprüft und aktiviert. Durch die Aktivierung gemäß Schritt **f** wird in der TA **8** ein Schlüsselpaar **11** generiert (Schritt **g**). Das Schlüsselpaar **11** wird dabei entweder in der TA8 bzw. der TEE des mobilen Endgeräts **2** selbst generiert oder bei einer fehlenden Funktionalität in der TEE durch den TAM **5** generiert und der TA **8** bereitgestellt. Während dem Schritt **g** wird zudem ein Zertifikat **14** für das Schlüsselpaar **11** beantragt (Schritt **h**) und dazu mittels des im QR-Code enthaltenen Verbindungsinformation eine Verbindung zur CA4 aufgebaut. Mittels des im QR-Code enthaltenen SCEP-OTP wird in der CA4 ein Zertifikat **14** erstellt, siehe Schritt **i** und das Zertifikat **14** an die TA **8** übertragen und optional in der TEE abgelegt (Schritt **j**). Im Schritt **e** oder nach dem Schritt **j** vergibt der Benutzer ein Zugangspasswort oder PIN für die TA **8**. Alternativ kann der Benutzer biometrische Sicherungsverfahren wie z.B. Fingerabdrücke verwenden.

[0083] Wenn im Schritt **b** die CP **9** noch nicht installiert wurde, so veranlasst die Registrierungsstelle **3** über den Verzeichnisdienst **14** die Installation nach dem Schritt **j**.

[0084] Gemäß einer ersten Ausführungsvariante des Verfahrens erstellt die CA **4** zudem ein Ersatz-Zertifikat, welches im Schritt **j'** in einem sicheren Speicherbereich des Endgeräts **1** kryptografisch gesichert abgelegt wird. Die kryptografischen Schlüssel für dieses Zertifikat werden auf dem Endgerät **1** erzeugt und für die Zertifikatserstellung an die CA **4** übertragen. Diese Beantragung kann über SCEP, oder ein anderes Verfahren erfolgen. Das Ersatz-Zertifikat wird bevorzugt im TPM des Endgeräts **1** abgelegt. Diese erste Ausführungsvariante wird dann angewendet, wenn eine Anmeldung am Endgerät **1** ausschließlich mittels eines Zertifikats ermöglicht werden soll.

[0085] Der Benutzer kann sich nun am Endgerät **1** mittels seines mobilen Endgeräts **2** anmelden. Dazu wird eine Bluetooth-LE Verbindung **6** zwischen dem Endgerät **1** und dem mobilen Endgerät **2** aufgebaut. Für die Einbettung in Windows™ sind eine Reihe von Bibliotheken zu verwenden, insbesondere die Standardschnittstellen „common application programming interface“ version 1 und 2, kurz: CAPI v1 & v2. Der CP **9** wird zusätzlich installiert, um den Anmeldeprozess des Endgeräts **1** für eine Authentifizierung mittels mobilem Endgerät **2** zu ermöglichen. Der CP **9** steuert und überwacht die Verbindung zum mobilen Endgerät **2**, sodass kein unsicherer Minitreiber benötigt wird, der es einem Angreifer ermöglichen könnte, die Kommunikation zwischen dem Endgerät **1** und dem mobilen Endgerät **2** zu unterbinden oder abzuhören.

[0086] Nach der erfolgreichen Anmeldung durch Authentifizierung des Benutzerzertifikats der TA **8** durch das Endgerät **1**, insbesondere dem zentralen Verzeichnisdienst **12**, wird im Schritt **aa** durch den CP **9** direkt ein OTP mit der Registrierungsstelle **3** ausgehandelt und (im Schritt **ab**) an diese Registrierungsstelle **3** gesendet und dort hinterlegt. Diese Übertragung im Schritt **ab** erfolgt verschlüsselt. Optional kann im Schritt **ac** auch das Ersatz-Zertifikat in der Registrierungsstelle **3** kryptografisch gesichert abgelegt werden. Das OTP bzw. das Ersatz-Zertifikat kann auch in dem Verzeichnisdienst **12** abgespeichert werden. Dieses OTP wird gemäß der Ausgestaltung der **Fig. 1** bis **Fig. 3** verwendet, um einen Benutzer an dem System anzumelden, sollte das mobile Endgerät **2** nicht vorhanden sein, wobei die Zwei-Faktor-Authentifizierung weiterhin eingehalten wird. Sollte in Schritt **aa** keine Verbindung zum Netzwerk **13** bestehen, wird dieser Schritt ausgeführt, wenn die Verbindung wieder hergestellt wurde.

[0087] In **Fig. 5** ist ein Ausführungsbeispiel eines Verfahrensablaufs zum erfindungsgemäßen Anmelden eines Benutzers an einem Endgerät **1** mittels mobilen Endgeräts **2** gezeigt. Dabei ist bevorzugt das in **Fig. 4** gezeigte Verfahren angewendet worden, um das System einzurichten.

[0088] Das Verfahren gemäß **Fig. 5** verwendet dabei ebenfalls das in den **Fig. 2** und **Fig. 3** gezeigte System.

[0089] Gemäß dem Schritt **k** ist ein gesperrtes Endgerät **1** vorgesehen, welches auf eine Benutzerauthentifizierung wartet, um entsperrt zu werden. Dabei ist auf dem Endgerät **1** der CP **9** installiert und ein OTP gemäß einer letztmaligen Anmeldung des Benutzers wurde hinterlegt.

[0090] Im Schritt **1** nähert sich der Benutzer dem Endgerät **1** mit seinem mobilen Endgerät **2**. Der Benutzer startet die TA **8** und gibt eine PIN ein, um die Authentifizierung zu starten. Es wird eine Bluetooth-Verbindung **6** zwischen dem Endgerät **1** und dem mobilen Endgerät **2** aufgebaut. Alternativ zur PIN können auch biometrische Sensoren Verwendung finden.

[0091] Im Schritt **m** erkennt das Endgerät **1** das mobile Endgerät **2** durch den installierten CP **9** und startet die Anmeldeprozedur aufgrund der gestarteten TA **8** im mobilen Endgerät **2**. Im Schritt **n** wird eine Verbindung zum Verzeichnisdienst **12** des Endgeräts **1** aufgebaut. Der Verzeichnisdienst **12** ist dabei eine Netzwerkkomponente des Netzwerks **13**. Ist die Verbindung zum Netzwerk nicht verfügbar wird versucht den Benutzer auf Basis der auf dem Endgerät **1** hinterlegten Daten zu authentifizieren (Offline-Anmeldung).

[0092] Im Schritt **o** generiert der Verzeichnisdienst **12** eine sogenannte Challenge beispielsweise gemäß dem Challenge Handshake Authentication Protocol, kurz CHAP. Das CHAP ist ein Authentifizierungsprotokoll. Im Schritt **n** initiiert das Endgerät **1** eine Verbindung zum Verzeichnisdienst **12**. Der Verzeichnisdienst erzeugt die Challenge im Schritt **o**. Die Challenge ist ein zufälliger Wert, der an das Endgerät **1** im Schritt **p** übertragen wird.

[0093] Das Endgerät **1** sendet die Challenge im Schritt **q** an das mobile Endgerät **2** via der BLE **6**. Die TA **8** signiert die Challenge im Schritt **u**. Das Signieren ist ein asymmetrisches Kryptoverfahren, bei dem das mobile Endgerät **2** mit Hilfe des geheimen Signaturschlüssels (dem Private Key) des Schlüsselpaars **11** zu der Challenge einen weiteren Wert berechnet.

[0094] Im Schritt **v** überträgt das mobile Endgerät **2** die signierte Challenge an das Endgerät **1** zurück. Das Endgerät **1** leitet die signierte Challenge im Schritt **w** an den Verzeichnisdienst **12** weiter.

[0095] Im Schritt **x** prüft der Verzeichnisdienst **12** die Signatur. Dazu wird der während der Signatur berechnete weitere Wert überprüft, indem mit Hilfe des öffentlichen Verifikationsschlüssels (dem Public Key) des Schlüsselpaars **11** die nicht-abstreitbare Urheberschaft und Integrität der Challenge verifiziert wird. Ggf. wird gemäß Schritt **y** auch die Gültigkeit des Zertifikats **14** in der Zertifizierungsstelle **4** abgefragt. Ist das Zertifikat **14** gültig und die Signatur korrekt, ist der Authentifizierungsversuch erfolgreich. Sodann wird das Endgerät **1** im Schritt **z** entsperrt und die Anmeldung des Benutzers mittels seines mobilen Endgeräts **2** ist erfolgt.

[0096] Nach der erfolgreichen Anmeldung wird - wie in den Schritten **aa** und **ab** der **Fig. 4** - im Schritt **aa** der **Fig. 5** durch den CP **9** ein neues OTP mit der Registrierungsstelle **3** ausgehandelt und (im Schritt **ab**) an diese Registrierungsstelle **3** und ggf. den Verzeichnisdienst **12** gesendet und dort abgelegt, sofern noch kein OTP existierte oder aus einem anderen Grund ein neues OTP erzeugt werden muss. Diese Übertragung im Schritt **ab** erfolgt verschlüsselt. Dieses neue OTP wird gemäß der Ausgestaltung der **Fig. 1** bis **Fig. 3** verwendet, um einen Benutzer an dem System anzumelden, sollte das mobile Endgerät **2** nicht vorhanden sein, wobei die Zwei-Faktor-Authentifizierung weiterhin eingehalten wird.

[0097] In den **Fig. 6** und **Fig. 7** werden nun zwei erfindungsgemäße Szenarien beschrieben, bei dem der Benutzer **16** sein mobiles Endgerät **2** nicht bei sich führt, beispielsweise weil er es verloren hat oder es defekt ist, er sich aber dennoch am Endgerät **1** über eine Zwei-Faktor-Authentifizierung anmelden sollte. Dazu sollte zumindest das Verfahren gemäß **Fig. 4** bereits abgeschlossen sein.

[0098] In **Fig. 6** ist im Schritt **ad** - wie im Schritt **k** in **Fig. 5** - das Endgerät **1** gesperrt und wartet auf eine Benutzerauthentifizierung, um entsperrt zu werden. Dabei ist auf dem Endgerät **1** der CP **9** installiert und ein OTP gemäß einer letztmaligen Anmeldung des Benutzers wurde hinterlegt. Im System gemäß **Fig. 6** ist eine Anmeldung eines Benutzers an einem Endgerät ausschließlich mittels eines Zertifikats möglich.

[0099] Der Benutzer kontaktiert im Schritt **ae** eine Auskunftsstelle **17**, und berichtet den Verlust/Defekt des mobilen Endgeräts **2**. Die Auskunftsstelle **17**, beispielsweise ein weiterer Teil der Registrierungsstelle **3** oder ein Helpdesk oder ein Teil im weiteren Server **15** oder eine andere Instanz im Netzwerk **13**, widerruft im Schritt **af** das bisherige Benutzerzertifikat **14** und fordert das OTP von der Registrierungsstelle **3** oder dem Verzeichnisdienst **12** im Schritt **ag** an. Das OTP wird dem Benutzer mündlich mitgeteilt, bspw. über eine Telefonverbindung. Alternativ kann das OTP auch über andere Geräte und Kommunikationsformen übertragen werden. Zudem wird der Anmeldevorgang im Endgerät **1** auf OTP-Eingabe umgestellt, beispielsweise automatisch durch den CP **9** oder eine Benutzereingabe in einer Anmelde-GUI. Der Benutzer gibt im Schritt **ah** das OTP am Endgerät **1** ein. Mittels dieses OTP wird ein Zugriff auf das Ersatz-Zertifikat im TPM des Endgeräts **1** freigeschaltet. Dieses Ersatz-Zertifikat wird anstelle des Benutzerzertifikats **14** verwendet, um die Challenge zu signieren. Es wird auf die Ausführungen zu **Fig. 1** verwiesen.

[0100] Die Schritte **n** bis **z** der **Fig. 6** entsprechen den Schritten **n** bis **z** gemäß der **Fig. 5**, wobei anstelle dem Benutzerzertifikat **14** des mobilen Endgeräts **2** nunmehr das Ersatz-Zertifikat des TPM des Endgeräts **1** verwendet wird.

[0101] Nach der erfolgreichen Anmeldung **z** wird - wie in den Schritten **aa** und **ab** der **Fig. 4** - im Schritt **aa** der **Fig. 6** durch den CP **9** direkt ein neues OTP mit der Registrierungsstelle **3** ausgehandelt und (im Schritt **ab**) an diese Registrierungsstelle **3** und den Verzeichnisdienst **12** gesendet und dort abgelegt. Diese Übertragung im Schritt **ab** erfolgt verschlüsselt. Dieses neue OTP wird gemäß der Ausgestaltung der **Fig. 1** bis **Fig. 3** verwendet, um einen Benutzer an dem Endgerät **1** anzumelden, sollte das mobile Endgerät **2** nicht vorhanden sein, wobei die Zwei-Faktor-Authentifizierung weiterhin eingehalten wird. Steht in Schritt **aa** die Verbindung zum Netzwerk nicht zur Verfügung wird dieser Schritt auf den Zeitpunkt verschoben, an dem die Verbindung wieder gegeben ist.

[0102] **Fig. 7** zeigt ein zweites erfindungsgemäßes Ausführungsbeispiel zur Anmeldung an einem Endgerät **1** ohne Vorhandensein des mobilen Endgeräts **2**. In **Fig. 7** ist - wie im Schritt **k** in **Fig. 5** - im Schritt **ad** das Endgerät **1** gesperrt und wartet auf eine Benutzerauthentifizierung, um entsperrt zu werden. Dabei ist auf dem Endgerät **1** der CP **9** installiert und ein OTP gemäß einer letztmaligen Anmeldung des Benutzers wurde hinterlegt. Im System gemäß **Fig. 7** ist - im Gegensatz zu **Fig. 6** - eine Anmeldung eines Benutzers an einem Endgerät auch ohne Zertifikat möglich, wobei dennoch eine Zwei-Faktor-Authentifizierung realisiert werden muss.

[0103] Der Benutzer kontaktiert im Schritt **ae** eine Auskunftsstelle **17**, und berichtet den Verlust/Defekt des mobilen Endgeräts **2**. Die Auskunftsstelle **17**, beispielsweise ein weiterer Teil der Registrierungsstelle **3** oder ein Helpdesk oder ein Teil im weiteren Server **15** oder eine andere Instanz im Netzwerk **13**, widerruft im Schritt **af** das bisherige Benutzerzertifikat **14** und fordert das OTP von der Registrierungsstelle **3** oder dem Verzeichnisdienst **12** im Schritt **ag** an. Das OTP wird dem Benutzer mündlich mitgeteilt, bspw. über eine Telefonverbindung. Zudem wird der Anmeldevorgang im Endgerät **1** auf OTP-Eingabe umgestellt, beispielsweise automatisch durch den CP **9** oder eine Benutzereingabe in einer Anmelde-GUI. Der Benutzer gibt im Schritt **ah** das OTP am Endgerät **1** ein. Bei erfolgreicher Eingabe wird nun im Schritt **ai** eine Anmeldemaske dargestellt und der Benutzer **16** aufgefordert, einen Benutzernamen und ein weiteres Passwort einzugeben. Diese Form der Anmeldung entspricht dem konventionellen Anmelden an einem Endgerät **1**. Dieser Benutzername und das weitere Passwort werden anstelle des Benutzerzertifikats **14** verwendet, um sich am Verzeichnisdienst **12** anzumelden. Alternativ zur manuellen Eingabe können die Informationen Benutzername und weiteres Passwort im geschützten Speicherbereich des Endgeräts (TPM) abgelegt werden und von dort unter Verwendung des OTP als Sicherungsmechanismus abgerufen werden. Dies ermöglicht die Nutzung weitaus komplexerer Passwörter, da der Benutzer sich dieses nicht merken muss.

[0104] Nach der erfolgreichen Anmeldung **z** wird - wie in den Schritten **aa** und **ab** der **Fig. 4** - im Schritt **aa** der **Fig. 6** durch den CP **9** direkt ein neues OTP mit der Registrierungsstelle **3** ausgehandelt und (im Schritt **ab**) an diese Registrierungsstelle **3** und den Verzeichnisdienst **12** gesendet und dort abgelegt. Diese Übertragung im Schritt **ab** erfolgt verschlüsselt. Dieses neue OTP wird gemäß der Ausgestaltung der **Fig. 1** bis **Fig. 3** verwendet, um einen Benutzer an dem Endgerät **1** anzumelden, sollte das mobile Endgerät **2** nicht vorhanden sein, wobei die Zwei-Faktor-Authentifizierung weiterhin eingehalten wird. Im Anschluss an diese Szenarien gemäß **Fig. 6** oder **Fig. 7** erhält der Benutzer ein neues mobiles Endgerät. Die Registrierungsstelle sendet erneut QR-Codes, um ein SCEP-OTP und Verbindungsinformationen zur CA **4** und dem TAM **5** an das neue mobile Endgerät **2** zu übertragen. Der Vorgang gleicht dem Schritt **d**) der **Fig. 4**. Die Schritte **e**) bis j)

gemäß der **Fig. 4** werden ebenfalls durchgeführt, auf eine Wiederholung wird aufgrund gleicher Vorgänge in den Schritten **e**) bis j) verzichtet. Ebenfalls wird gemäß der Schritte **aa** und **ab** ein neues OTP generiert und in der Registrierungsstelle **3** und /oder dem Verzeichnisdienst **12** hinterlegt.

[0105] Nachfolgend wird ein Szenario beschrieben, bei dem der Benutzer im System gemäß der **Fig. 2** und **Fig. 3** und des Ablaufs gemäß der **Fig. 4** bei einer vergessenen PIN für die TA **8** und somit die TA **8** gesperrt bleibt. Dabei kontaktiert der Benutzer die Auskunftsstelle, welche ein neues Benutzerzertifikat bei der Registrierungsstelle **3** beauftragt. Die Registrierungsstelle **3** fordert sodann eine Benutzerzertifikats-Aktualisierung bei der CA **4** an, woraufhin die Schritte **d**) und e) wiederholt werden und im Rahmen des Schritts **e**) ein neuer PIN durch den Benutzer vergeben werden kann. Nachfolgend wird wiederum ein neues OTP gemäß der Schritte **aa** und **ab** der **Fig. 4** oder **Fig. 5** erzeugt und abgelegt. Das Zurücksetzen der PIN erfolgt alternativ über ein hierarchisch übergeordnetes Passwort, beispielsweise einer PUK.

[0106] Im Rahmen der Erfindung können alle beschriebenen und/oder gezeichneten und/oder beanspruchten Elemente beliebig miteinander kombiniert werden.

Bezugszeichenliste

1	Endgerät
2	Mobiles Endgerät
3	Registrierungsstelle, Selbstverwaltungsportal
4	Zertifizierungsstelle, CA, Certification Authority
5	Sicheranwendungsverwaltung, TAM, Trusted Application Manager
6	Drahtlos-Verbindung, Bluetooth LE
7	Lizenzvergabestelle, TLS
8	Sichere Anwendung
9	Berechtigungsanfrage-Routine, Credential Provider, CP
10	Registrierungsanwendung
11	Schlüsselpaar für Benutzerzertifikat
12	Verzeichnisdienst, AD
13	Netzwerk
14	Benutzerzertifikat
15	Weitere Server-Dienste, bspw. Card-Management-Dienst
16	Benutzer
a, a'	Freischalten des Benutzers
b	Installieren des CP
c	Installieren der sicheren Anwendung
d	Generieren Zugang zu CA und TAM
e	Einrichten der sicheren Anwendung (Zugang + PIN), QR
f	Aktivieren der sicheren Anwendung
g	Generieren eines kryptografischen Schlüssels
h	Generieren eines Zertifikatsantrags
i	Zertifikat erstellen
j	Zertifikat ablegen
k	Endgerät im gesperrten Zustand
1	Starten der sicheren Anwendung und Verbindungsaufbau zum Endgerät
m	Credential Provider startet Anmeldeprozedur
n	Info an TAM
o	Generieren einer Berechtigungsaufforderung, Challenge
p	Challenge an Endgerät
q	Challenge an sichere Anwendung
u	Signieren der Challenge
v	Signierte Challenge an Endgerät
w	Signierte Challenge an TAM
x	Prüfung Zertifikat und Signatur, Benutzerberechtigung
y	Prüfung Gültigkeit des Zertifikats
z	Entsperren des Endgeräts
aa	Generieren eines Fallback-OTP
ab	Speichern des Fallback-OTP
ac	Speichern eines Ersatz-Zertifikats
ad	Endgerät im gesperrten Zustand
ae	Kontaktieren der Auskunftsstelle
af	Widerruf des Benutzerzertifikats
ag	Anfordern des OTP
ah	Eingabe des OTP beim Endgerät
ai	Darstellen einer (konventionellen) Anmeldemaske

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

- US 7783702 B2 [0008]
- US 2014/0068723 A1 [0009]
- US 8646060 B2 [0010]
- US 2015/0121068 A1 [0012]
- US 2016/0330199 A1 [0013]

Patentansprüche

1. Verfahren zum Authentifizieren eines Benutzers an einem Endgerät (1) mittels eines mobilen Endgeräts (2), wobei das Verfahren die folgenden Schritte umfasst:
- Einrichten (e) einer sicheren Anwendung (8) auf dem mobilen Endgerät (2);
- Verbinden (f) der sicheren Anwendung (8) zu einem Verwaltungssystem (5) zum Aktivieren der sicheren Anwendung (8);
- Anfragen und Erhalten (h, i, j) eines neuen Benutzerzertifikats bei einer Zertifizierungsstelle (4) durch die aktivierte sichere Anwendung (8);
- Starten (1) der sicheren Anwendung (8) auf dem mobilen Endgerät (2) und Aufbauen einer drahtlosen Kommunikationsverbindung vom mobilen Endgerät (2) zu dem Endgerät (1);
- Starten (m) der Berechtigungsanfrage-Routine (9) im Endgerät (1) und Aufbau einer Kommunikationsverbindung zum Netzwerk (13) oder einem Verzeichnisdienst (12) zur Authentifizierung des Benutzers;
- Generieren (o) einer Berechtigungsaufforderung durch das Netzwerk (13) oder den Verzeichnisdienst (12) und Übertragen (p) dieser an das Endgerät (1);
- Signieren (u) der Berechtigungsaufforderung mittels des Benutzerzertifikats (14) in der sicheren Anwendung (8);
- Übertragen (w) der signierten Berechtigungsaufforderung an das Netzwerk (13) oder den Verzeichnisdienst (12) zum Prüfen (x) der Signatur, bevorzugt unter Prüfen (y) der Gültigkeit des Benutzerzertifikats (14) ;
- Erteilen (z) einer Anmelde-Erlaubnis vom Netzwerk (13) oder dem Verzeichnisdienst (14) bei erfolgreicher Prüfung (x, y);
- Generieren (aa) eines Einmal-Passworts durch die Berechtigungsanfrage-Routine (9) des Endgeräts (1) ; und
- Speichern (ab) des Einmal-Passworts bei einer Registrierungsstelle (3) und/oder einem Anmeldedienst.

2. Verfahren nach Anspruch 1, wobei für den Verbinden-Schritt (f) Informationen von der Registrierungsstelle (3) zum Erzeugen einer Verbindung zum Verwaltungssystem (5) in der sicheren Anwendung (8) erhalten werden und diese Informationen als QR-Code bereitgestellt (d) und mittels einer Kamera des mobilen Endgeräts (2) erfasst (e) werden.

3. Verfahren nach Anspruch 2, wobei die Informationen von der Registrierungsstelle (3) zudem Verbindungsinformationen für die Zertifizierungsstelle (4) beinhalten.

4. Verfahren nach einem der vorhergehenden Ansprüche, wobei die sichere Anwendung (8) in einer sicheren Laufzeitumgebung des mobilen Endgeräts (2) abläuft und das Benutzerzertifikat (14) für ein kryptografisches Schlüsselpaar (11) generiert wird, das in einem nur für die sichere Laufzeitumgebung zugreifbaren sicheren Speicherbereich des mobilen Endgeräts (2) abgelegt ist.

5. Mobiles Endgerät (2) zum Authentifizieren eines Benutzers an einem Endgerät (1) eines Netzwerks gemäß einem der vorhergehenden Ansprüche aufweisend:
- eine gesicherte Laufzeitumgebung beinhaltend die sichere Anwendung (8);
- ein Drahtlosverbindungsmodul (6), insbesondere Bluetooth LE Modul, eingerichtet zur Kommunikation mit einer Berechtigungsanfrage-Routine (9) eines Endgeräts (1);
- ein Drahtlosverbindungsmodul, insbesondere Mobilfunk- oder Breitbandverbindungsmodul, eingerichtet zur Kommunikation mit einer Zertifizierungsstelle (4) zum Erhalten eines Benutzerzertifikats (14);
- einem Speicherbereich zum gesicherten Ablegen eines Schlüsselpaares (11), wobei die gesicherte Laufzeitumgebung eingerichtet ist, exklusiv auf den Speicherbereich zuzugreifen; und
- eine Kamera zum Erfassen von Informationen einer Registrierungsstelle.

6. Computerprogrammprodukt, ausführbar in einer sicheren Laufzeitumgebung eines mobilen Endgeräts (2) und eingerichtet zum Authentifizieren eines Benutzers an einem Netzwerk (13), wobei dazu das Verfahren nach einem der Ansprüche 1 bis 4 durchgeführt wird.

7. Computerprogrammprodukt, ausführbar in einem Endgerät (1) eines Netzwerks (13) und eingerichtet zum Abfragen einer Berechtigung eines Benutzers, wobei dazu das Verfahren nach einem der Ansprüche 1 bis 4 durchgeführt wird.

Es folgen 7 Seiten Zeichnungen

Anhängende Zeichnungen

100

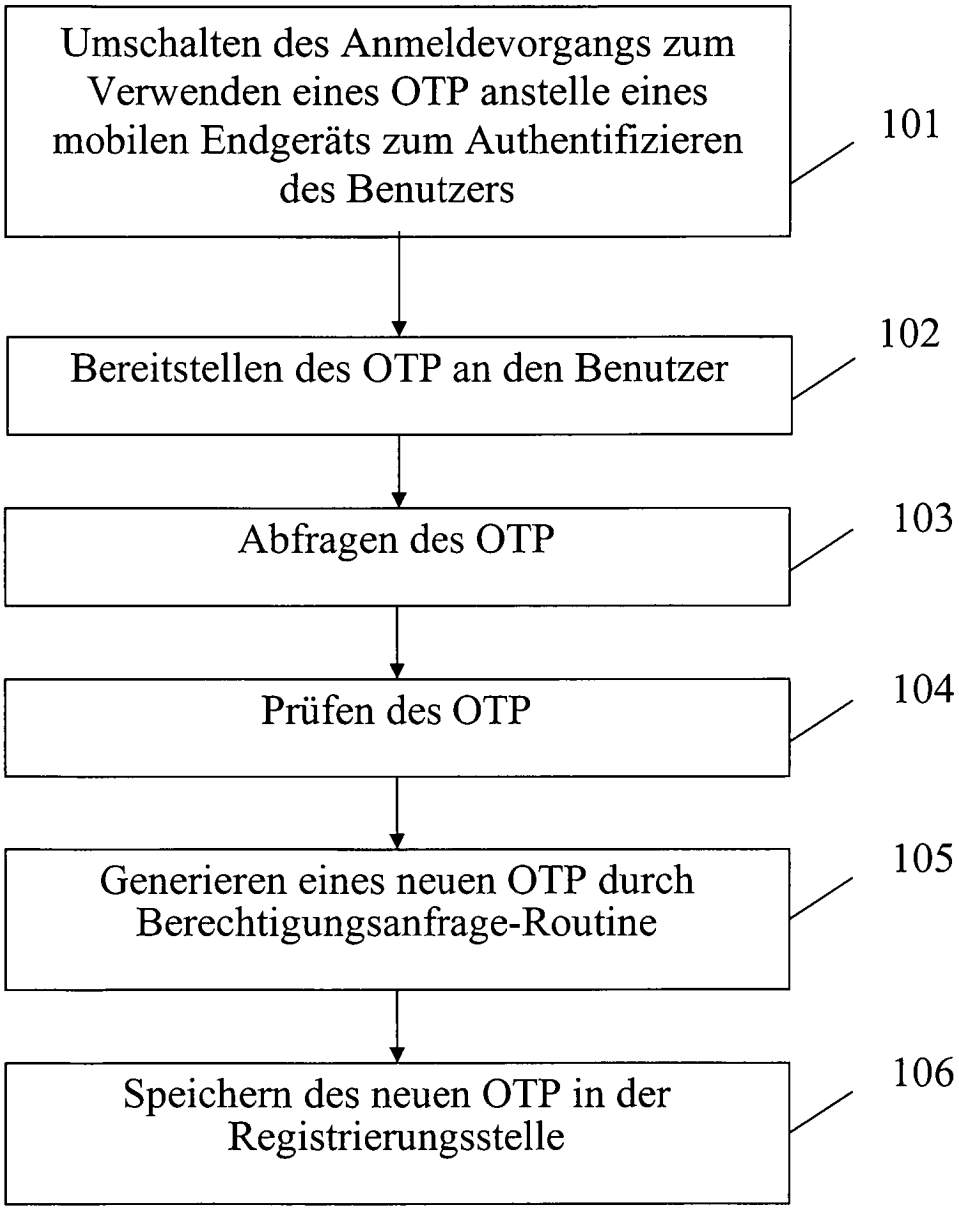


Fig. 1

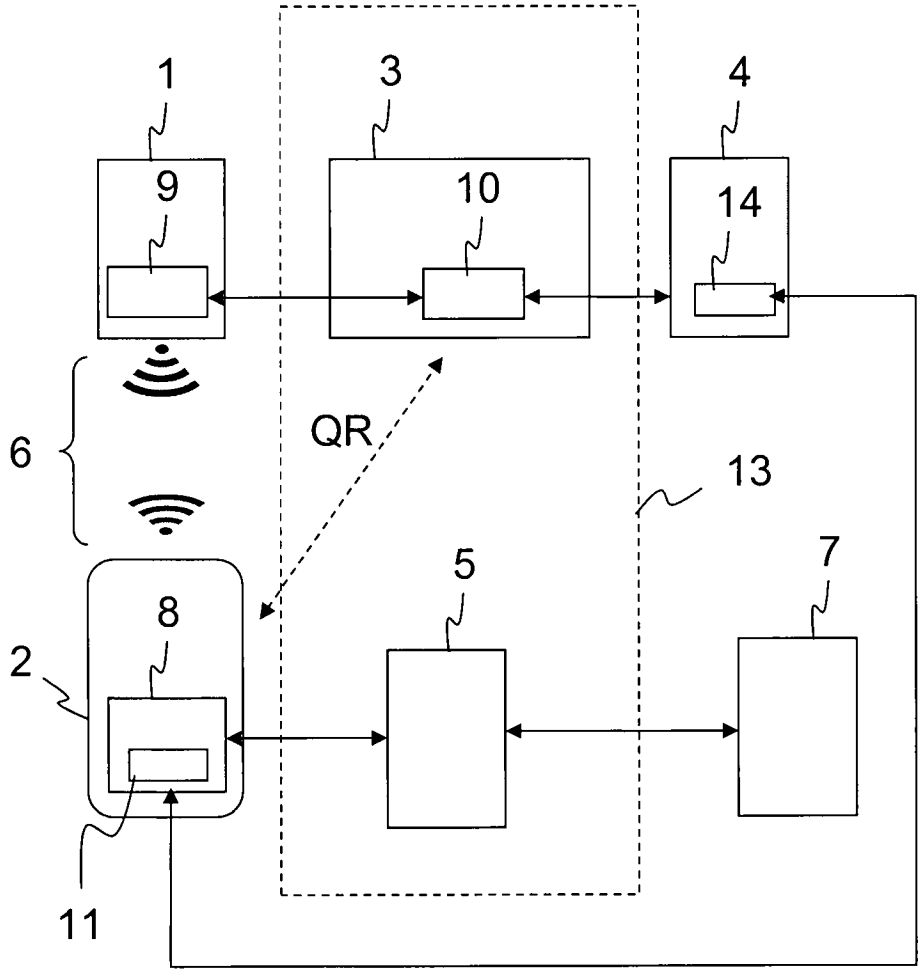


Fig. 2

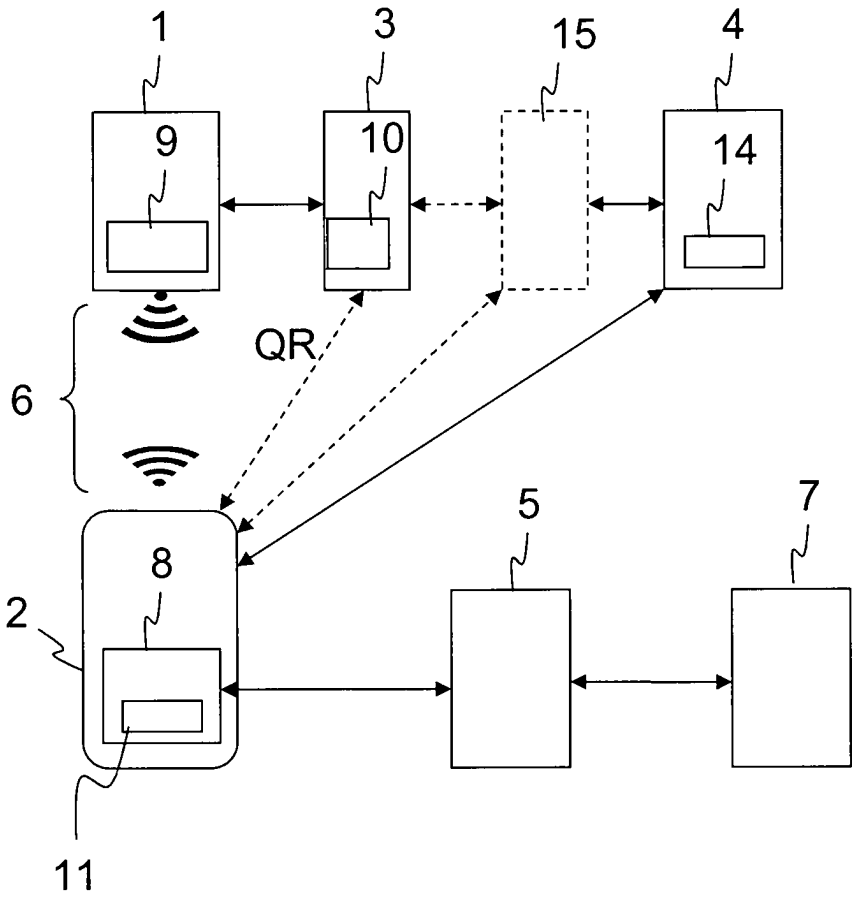


Fig. 3

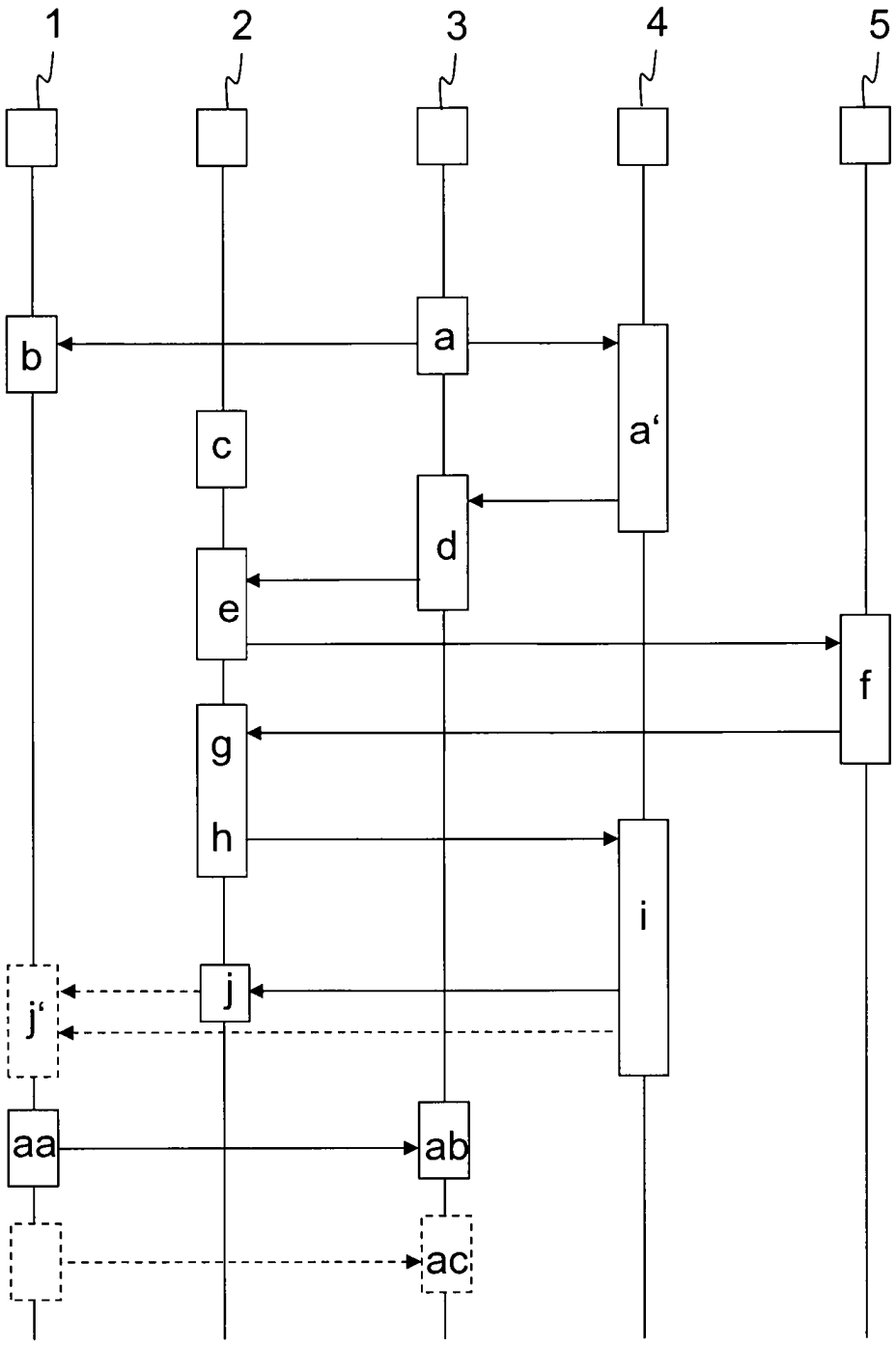


Fig. 4

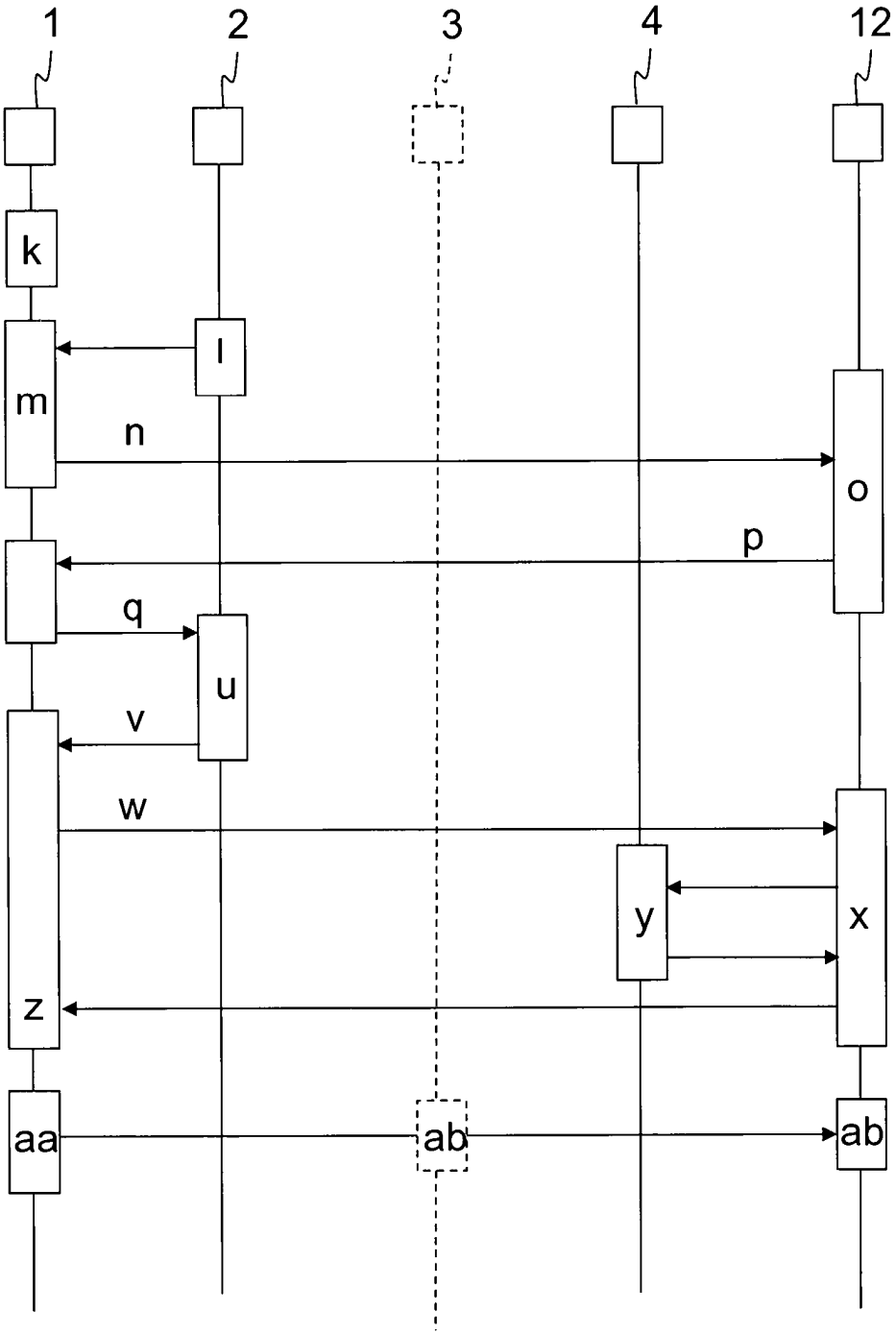


Fig. 5

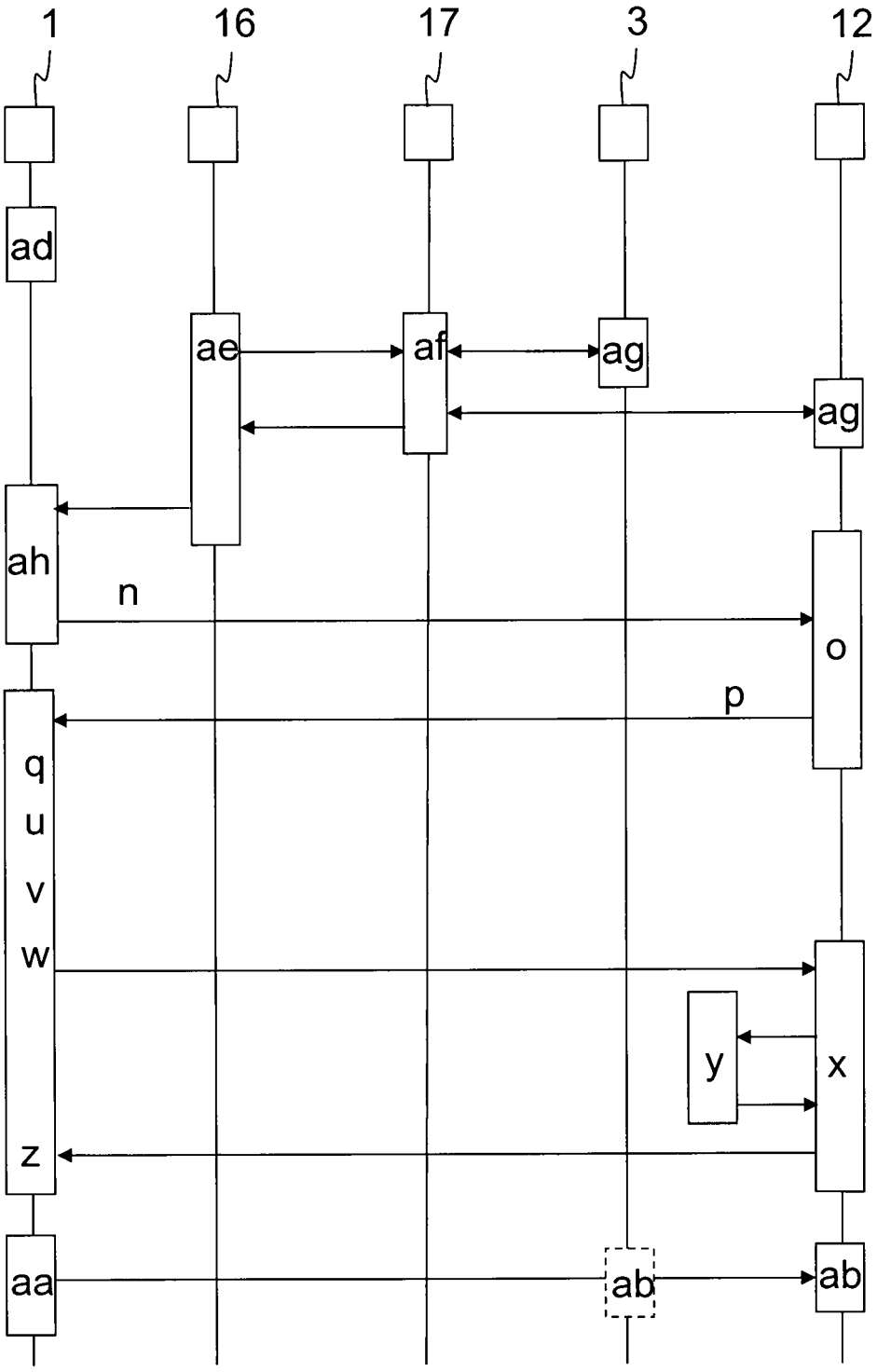


Fig. 6

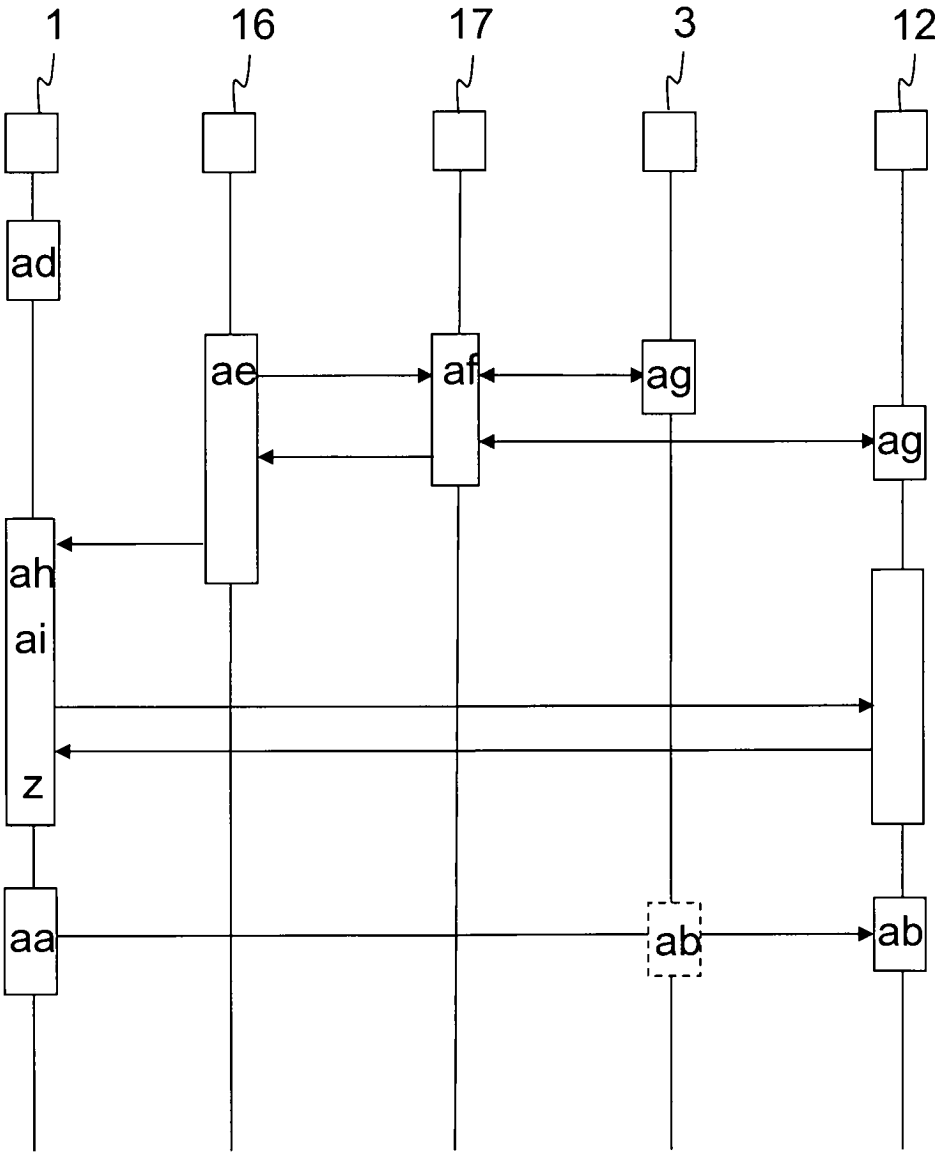


Fig. 7