

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges
Eigentum

Internationales Büro

(43) Internationales
Veröffentlichungsdatum
27. August 2015 (27.08.2015)



(10) Internationale Veröffentlichungsnummer
WO 2015/124726 A1

(51) Internationale Patentklassifikation:
H04L 9/32 (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2015/053622

(22) Internationales Anmeldedatum:
20. Februar 2015 (20.02.2015)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2014 102 168.1
20. Februar 2014 (20.02.2014) DE

(71) Anmelder: **PHOENIX CONTACT GMBH & CO. KG**
[DE/DE]; Flachsmarktstrasse 8, 32825 Blomberg (DE).

(72) Erfinder: **NITSCHKE, Torsten**; Genfer Weg 6, 44287
Dortmund (DE).

(74) Anwalt: **BLUMBACH & ZINNGREBE**;
Alexandrastrasse 5, 65187 Wiesbaden (DE).

(81) Bestimmungsstaaten (soweit nicht anders angegeben, für
jede verfügbare nationale Schutzrechtsart): AE, AG, AL,
AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW,

BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK,
DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM,
GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP,
KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME,
MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ,
OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA,
SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM,
TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM,
ZW.

(84) Bestimmungsstaaten (soweit nicht anders angegeben, für
jede verfügbare regionale Schutzrechtsart): ARIPO (BW,
GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST,
SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG,
KZ, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH,
CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE,
IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO,
RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM,
GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

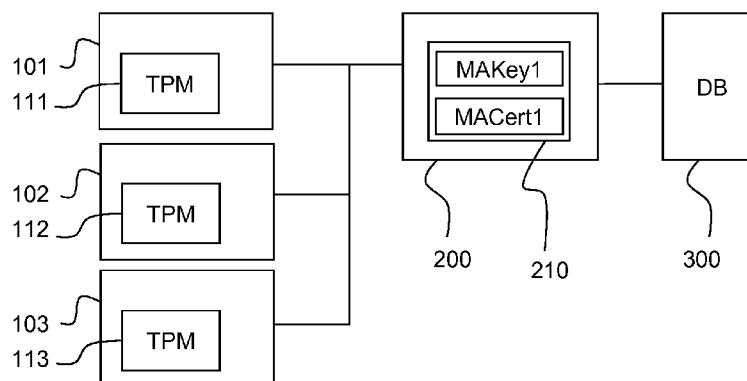
Veröffentlicht:

— mit internationalem Recherchenbericht (Artikel 21 Absatz
3)

(54) Title: METHOD AND SYSTEM FOR CREATING AND CHECKING THE VALIDITY OF DEVICE CERTIFICATES

(54) Bezeichnung : VERFAHREN UND SYSTEM ZUM ERSTELLEN UND ZUR GÜLTIGKEITSPRÜFUNG VON
GERÄTEZERTIFIKATEN

Fig. 1



(57) Abstract: In order to easily identify an invalid device certificate by means of a validity check when signing keys that are used to create device certificates are compromised, the invention proposes providing a piece of state information for device certificates that comprises positive evidence of the existence and validity of the device certificate, and alternatively or additionally applying a special validity model for device certificates, wherein the time of issue of the device certificate is documented by means of a signed electronic timestamp, wherein a different signing key is used for signing the timestamp than for signing the device certificate. A further aspect of the invention involves all information that is required for the validity check on a device certificate being stored in a memory of the device or in a memory associated with the device, so that an identity check on the device can be performed at any time without fetching additional data, i.e. an offline check on the stored device certificate is made possible.

(57) Zusammenfassung:

[Fortsetzung auf der nächsten Seite]



Um für den Fall der Kompromittierung von Signierschlüsseln, die zur Erstellung von Gerätezertifikaten verwendet werden, auf einfache Weise ein ungültiges Gerätezertifikat durch eine Gültigkeitsprüfung zu erkennen, schlägt die Erfindung vor, eine Zustandsauskunft für Gerätezertifikate bereitzustellen, welche einen Positivnachweis der Existenz und Gültigkeit des Gerätezertifikates umfasst, sowie alternativ oder zusätzlich ein spezielles Gültigkeitsmodell für Gerätezertifikate anzuwenden, wobei der Ausstellungszeitpunkt des Gerätezertifikates mittels eines signierten elektronischen Zeitstempels dokumentiert wird, wobei zum Signieren des Zeitstempels ein anderer Signierschlüssel eingesetzt wird als zum Signieren des Gerätezertifikates. Ein weiterer Aspekt der Erfindung besteht darin, alle für die Gültigkeitsprüfung eines Gerätezertifikates erforderlichen Informationen in einem Speicher des Gerätes oder in einem dem Gerät zugeordneten Speicher zu speichern, so dass jederzeit eine Identitätsprüfung des Gerätes ohne Einholen zusätzlicher Daten erfolgen kann, d.h. eine Offline-Prüfung des gespeicherten Gerätezertifikates ermöglicht wird.

Verfahren und System zum Erstellen und zur Gültigkeitsprüfung von Gerätezertifikaten

5 Beschreibung

Die Erfindung betrifft allgemein Gerätezertifikate, d.h. elektronische Zertifikate zur Bestätigung der Identität eines Gerätes, und insbesondere jeweils ein Verfahren und
10 ein System zum Erstellen von Gerätezertifikaten und zur Gültigkeitsprüfung von Gerätezertifikaten.

Elektronische Zertifikate dienen der Bestätigung von Informationen, insbesondere bestimmter Eigenschaften von
15 Personen oder Objekten, auf eine Weise, die eine Authentizitäts- und Integritätsprüfung mittels kryptografischer Verfahren erlaubt, wobei das Zertifikat in der Regel die zur Prüfung erforderlichen Daten beinhaltet.

20 Insbesondere wird ein elektronisches Zertifikat von einer ausstellenden Zertifizierungsinstanz digital signiert, wobei die digitale Signatur Bestandteil des Zertifikates ist. Häufig wird aus den zu zertifizierenden Informationen eine kryptografische Prüfsumme gebildet, zum Beispiel
25 mittels einer Hash-Funktion, und nur diese Prüfsumme mit dem privaten Anteil eines asymmetrischen Schlüsselpaares der Zertifizierungsinstanz digital signiert. Auf diese Weise kann mittels des öffentlichen Schlüssels der Zertifizierungsinstanz die Authentizität der zertifizierten
30 Informationen überprüft werden, indem unter Verwendung des Public-Key-Verfahrens die ursprüngliche kryptografische Prüfsumme ermittelt und mit einer aus den zertifizierten Informationen erneut gebildeten kryptografischen Prüfsumme

verglichen wird, wobei bei Übereinstimmung der kryptografischen Prüfsummen die Authentizität der zertifizierten Informationen vorliegt.

- 5 Die rechtliche Gültigkeit elektronischer Signaturen wird in Deutschland durch das Signaturgesetz und die Signaturverordnung geregelt, wobei per Gesetz qualifizierte elektronische Signaturen rechtlich handschriftlichen Unterschriften mit wenigen Ausnahmen gleich gestellt sind.
- 10 Für qualifizierte elektronische Signaturen bestehen bestimmte Anforderungen an den Signaturerstellungsprozess, die dabei verwendeten Mittel und insbesondere an die Zertifizierungsdienste, welche die dafür notwendigen qualifizierten Zertifikate ausstellen. Qualifizierte
- 15 elektronische Signaturen werden immer von natürlichen Personen erstellt. Entsprechend ist der Inhaber eines qualifizierten elektronischen Zertifikates für Signaturen immer eine natürliche Person.
- 20 Zur Bestätigung der Identität eines Gerätes werden als Gerätezertifikate bezeichnete elektronische Zertifikate eingesetzt, wobei Gerätezertifikate unter anderem dazu dienen, einem Gerätebesitzer die Prüfung der Echtheit eines Gerätes zu ermöglichen. Ein Zertifikat mit diesem Zweck
- 25 wird als Echtheitszertifikat bezeichnet. Außerdem kann ein Gerätebesitzer selbst ausgestellte Gerätezertifikate zur Kennzeichnung seines Besitzes verwenden. Solche Zertifikate werden als Besitzzertifikate bezeichnet.
- 30 Ein Echtheitszertifikat ist dementsprechend ein Gerätezertifikat, das von einem Gerätehersteller zur Bestätigung der Echtheit eines von ihm hergestellten

Gerätes erstellt wurde. Echtheit bedeutet in diesem Zusammenhang, dass ein Gerät tatsächlich von einem bestimmten Hersteller stammt. Ein Gerätehersteller stellt dazu bei der Herstellung des Gerätes ein Zertifikat für ein
5 einmaliges, nur in dem Gerät befindliches Geheimnis aus. Der Gerätehersteller veröffentlicht die Prüfkriterien für diese Zertifikate, damit ein Besitzer die Echtheit der Geräte bestimmen kann.

10 Solche Zertifikate sind in einschlägiger Literatur beschrieben. So wird beispielsweise im IEEE Standard 802.1AR -2009 (IEEE Standard for Local and metropolitan area networks - Secure Device Identity, 2009) ein sogenannter Initial Secure Device Identifier (IDevID)
15 beschrieben, bestehend aus einem Geheimnis in Form eines privaten Schlüssels und einem Zertifikat in Form eines Public-Key-Zertifikats konform zu dem in RFC 5280 (Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile) beschriebenen X.509-
20 Zertifikat. Für die X.509 Public Key Infrastructure wird nachfolgend auch die Kurzbezeichnung PKIX verwendet.

Ferner beschreibt die Spezifikation des Trusted Platform Module (TPM) der Trusted Computing Group unter anderem in
25 Teil 1 (TPM Main Part 1 Design Principles Specification Version 1.2, Revision 116, 1. März 2011, TCG) einen sogenannten "Endorsement Key" bestehend aus einem asymmetrischen Schlüsselpaar, umfassend einen als PRIVEK bezeichneten privaten Schlüssel und einen als PUBEK
30 bezeichneten öffentlichen Schlüssel, zu dem Zwecke, die Echtheit des TPM-Chips mittels elektronischer Signatur, zum Beispiel mittels Zertifikat, zu bestätigen. Ein

entsprechendes Zertifikat wird im Folgenden auch als EK-Zertifikat bezeichnet.

Ein Endorsement Key (EK) eines TPM-Chips kann mit Hilfe
5 eines öffentlich bekannten Wurzelzertifikates überprüft
werden. Ferner können Plattformhersteller, wie zum Beispiel
Platinen- oder Gerätehersteller, welche ein TPM
integrieren, ein als „Platform Endorsement Certificate“
bezeichnetes Attributzertifikat erstellen, um die
10 Integration eines TPM-Chips mit einmaligem Endorsement Key
in eine bestimmte Plattform zu bestätigen.
Aus dem Stand der Technik ist somit bekannt, die
Herstellung von Geräten und deren Echtheit mittels
elektronischer Unterschriften zu dokumentieren und durch
15 den späteren Gerätebesitzer prüfbar zu machen.

In der Regel sind dazu beim Gerätehersteller asymmetrische
Schlüsselpaare, im Folgenden auch als Manufacturer's
Attestation Keys (MAKey) bezeichnet, im Einsatz. Das zum
20 MAKey gehörende, als MACert bezeichnete Zertifikat wird in
der Regel im Range eines sogenannten Zwischenzertifikates
(intermediate CA certificate, Sub-CA-Zertifikat) einer
Zertifizierungsstelle als Bestandteil einer
Zertifikatskette verwendet. Dieses Zertifikat ist direkt
25 oder indirekt durch die Zertifizierungsstelle des
Herstellers bestätigt, zum Beispiel indem der als
Manufacturer's Trust Anchor Key, kurz MTAKey, bezeichnete
Wurzelschlüssel der Zertifizierungsstelle verwendet wurde,
um es digital zu signieren. Der Wurzelschlüssel wird in der
30 Regel mit Hilfe eines selbst-signierten Wurzelzertifikates,
auch als Manufacturer's Trust Anchor Certificate, kurz

MTACert, bezeichnet, bestätigt und vom Hersteller veröffentlicht.

Der private Anteil des MAKeys wird an einem
5 Produktionsarbeitsplatz verwendet. Sollte solch ein privater Anteil kopiert oder missbraucht werden, können originale Gerätezertifikate nicht von missbräuchlich erstellten Gerätezertifikaten unterschieden werden. In solchen Fällen wird das zugehörige Sub-CA-Zertifikat
10 üblicherweise gesperrt. Damit diese Wirksamkeit zeigt, müssen während der Prüfung von Zertifikatsketten noch zusätzlich Sperrinformationen eingeholt werden. Sperrinformationen werden üblicherweise durch regelmäßige Veröffentlichung einer Certificate Revocation List (CRL)
15 oder relativ unverzüglich über Sperrinformationsdienste wie einen OCSP-Server (Online Certificate Status Protocol Server), beispielsweise gemäß RFC 2560, zur Verfügung gestellt.

20 Während der Verifikation einer Zertifikatskette müssen gemäß RFC 5280 die Gültigkeitszeiträume der Zertifikate beachtet werden. Dies gilt besonders, wenn Sperrinformationen zu beachten sind. Die Gültigkeit einer Zertifikatskette wird bei dem in RFC 5280 beschriebenen
25 Verfahren für einen bestimmten Zeitpunkt t , in der Regel für die aktuelle Zeit, überprüft. Der Zeitpunkt t muss innerhalb des Gültigkeitszeitraumes aller Zertifikate der Kette liegen und für alle Zertifikate der Kette außer dem Wurzelzertifikat müssen Sperrinformationen vorliegen, die
30 gemessen an t hinreichend jung und gültig sind, wobei Sperrinformationen in der Regel ebenfalls einen Gültigkeitszeitraum nennen.

Eine Sperrung eines Sub-CA-Zertifikates hat zur Folge, dass alle bereits ausgestellten und damit zu prüfenden Gerätezertifikate ungültig werden. Als Gegenmaßnahme muss
5 ein Gerätehersteller anhand seiner Gerätedatenbank neue Gerätezertifikate für die betroffenen Geräte ausstellen, bei Verwendung von TPMs beispielsweise in Form von EK-Zertifikaten,. Aus diesem Grunde sind bei der Herstellung der Geräte die öffentlichen Teile eingesetzter
10 asymmetrischer Schlüsselpaare, wie beispielsweise eines Endorsement Key (EK), in einer Gerätedatenbank zu archivieren. Allerdings ist die Ausstellung neuer Gerätezertifikate mit Aufwand und Kosten verbunden, insbesondere dann, wenn die Geräte im Feld schwierig oder
15 nicht erreichbar sind.

Wegen der Kosten im Falle einer Kompromittierung von privaten Schlüsseln, die zu Sub-CA-Zertifikaten gehören, wird in der Praxis häufig auf die Sperrung von Sub-CA-
20 Zertifikaten verzichtet und es werden gegebenenfalls kaufmännische Maßnahmen zur Regelung von Schäden angewendet. Oftmals bestehen keine Prozeduren, nach denen im Falle einer Kompromittierung zu handeln ist.

25 Ein weiteres Problem besteht darin, dass die Sperrinformation am Ort der Prüfung verfügbar gemacht werden muss, je nach Einsatzzweck jedoch am Ort der Prüfung gegebenenfalls keine Verbindung zu einem Kommunikationsnetzwerk zur Verfügung steht.

30

Ein Besitzzertifikat ist ein Gerätezertifikat, welches von einem Gerätebesitzer für sein Gerät ausgestellt wird, um zu

bestätigen, dass es sich in seinem Besitz befindet, und stellt somit ein Identifikationskriterium für seinen Besitz dar. Ein Gerätebesitzer stellt dazu bei der Inbesitznahme eines Gerätes und gegebenenfalls auch wiederholt während
5 des Besitzes ein Zertifikat für ein einmaliges, nur in dem Gerät befindliches Geheimnis aus. Der Gerätebesitzer verwendet die zum Zertifikat gehörenden Prüfkriterien um jederzeit effizient feststellen zu können, ob ein Gerät zu seinem Besitz gehört oder nicht. Weiter verwenden die
10 Geräte des Besitzers diese Zertifikate untereinander, um sich gegenseitig ihre Identität und Zugehörigkeit zur Vertrauensdomäne des Besitzers nachzuweisen.

Aus dem Dokument RFC 5916 (Device Owner Attribute) der
15 Internet Engineering Task Force (IETF) ist beispielsweise ein Attribut für Public-Key-Zertifikate und Attributzertifikate bekannt, mit dem der Besitz eines Gerätes bezeichnet werden kann. Es nennt als Zweck für dieses Attribut zum Beispiel seine Verwendung bei einer
20 automatischen Entscheidung der Vertrauenswürdigkeit zwischen zwei miteinander kommunizierenden Geräten. Sie vertrauen sich beispielsweise, wenn ihre Zertifikate den entsprechenden Eigentümer nennen.

25 In der Regel verwenden Gerätehersteller für ihre Geräte Gerätezertifikate kompatibel zum PKIX-Standard, damit eine möglichst große Interoperabilität gewährleistet ist. Insbesondere wird das durch den PKIX-Standard definierte Gültigkeitsmodell für Zertifikatsketten angewendet.

30

Bei der Erstellung von Gerätezertifikaten verwenden manche Gerätebesitzer einen eigenen Zertifizierungsdienst, welcher

mit einem als Device Owner's Attestation Key (DOAKey) bezeichneten Schlüssel Gerätezertifikate unterzeichnet, wobei auch mehrere Schlüssel dieser Art (DOAKey1, DOAKey2, DOAKey3, ...) eingesetzt werden können. Analog zu den oben
5 beschriebenen Schlüsseln MAKey und MTAKKey bzw. Zertifikaten MACert und MTACert und mit analoger Verwendung sind in der Regel ein als Device Owner's Attestation Certificate (DOACert) bezeichnetes Zertifikat zu einem DOAKey, sowie ein als Device Owner's Trust Anchor Key (DOTAKey)
10 bezeichneter Schlüssel der Wurzelinstanz des Zertifizierungsdienstes und ein zugehöriges Zertifikat Device Owner's Trust Anchor Certificate (DOTACert) vorgesehen.

15 Der Unterschied zu den oben beschriebenen Schlüsseln MAKey und MTAKKey bzw. Zertifikaten MACert und MTACert ist, dass der Gerätebesitzer die Verwendung seiner Schlüssel und Zertifikate kontrolliert und das von ihm erzeugte Gerätezertifikat erst nach Erhalt des Gerätes erzeugt und
20 einbringt. Für das Gerätezertifikat wird entweder ein vorhandenes Schlüsselpaar des Gerätes verwendet, zum Beispiel der EK im TPM eines Gerätes, ein neues Schlüsselpaar im Gerät erzeugt, zum Beispiel mit Hilfe eines TPM, oder durch den Gerätebesitzer ein neues
25 Schlüsselpaar erzeugt und in das Gerät eingebracht.

Bei der Kompromittierung von Schlüsseln zur Ausstellung von Gerätezertifikaten (DOAKey1, DOAKey2, DOAKey3, ...) bestehen die gleichen Schwierigkeiten und Kosten für den
30 Gerätebesitzer wie sie oben für den Gerätehersteller beschrieben wurden. Bei einem Gültigkeitsmodell nach dem PKIX-Standard werden alle mit dem jeweiligen Schlüssel

unterzeichneten Gerätezertifikate ungültig und müssen ersetzt werden. Bei industriellen Geräten sind diese durchaus an unzugänglichen Stellen im Feld installiert, so dass der Austausch aufwändig ist.

5

Zudem besteht auch hier das oben beschriebene Problem, dass am Ort der Prüfung gegebenenfalls kein Zugang zu einem Kommunikationsnetzwerk zur Bereitstellung der Sperrinformationen besteht.

10

Es ist daher die Aufgabe der vorliegenden Erfindung, einen Weg aufzuzeigen, wie die oben beschriebenen Probleme im Stand der Technik reduziert oder vermieden werden können, und insbesondere einen Weg aufzuzeigen, wie die Erstellung und Gültigkeitsprüfung von Gerätezertifikaten vereinfacht und/oder verbessert werden kann, insbesondere für den Fall der Kompromittierung von Signierschlüsseln, die zur Erstellung von Gerätezertifikaten verwendet werden, sowie für den Fall, dass zum Zeitpunkt der Gültigkeitsprüfung keine Kommunikationsverbindung zur Verfügung steht.

20

Diese Aufgabe wird durch die Merkmale der unabhängigen Ansprüche gelöst. Vorteilhafte Ausführungsformen sind Gegenstand der abhängigen Ansprüche.

25

Ein Grundgedanke der Erfindung besteht darin, eine Zustandsauskunft für Gerätezertifikate bereitzustellen, welche einen Positivnachweis der Existenz und Gültigkeit des Gerätezertifikates umfasst, sowie alternativ oder zusätzlich ein spezielles Gültigkeitsmodell für Gerätezertifikate anzuwenden, wobei der Ausstellungszeitpunkt des Gerätezertifikates mittels eines

30

signierten elektronischen Zeitstempels dokumentiert wird, wobei zum Signieren des Zeitstempels ein anderer Signierschlüssel eingesetzt wird als zum Signieren des Gerätezertifikates.

5

Ein weiterer Aspekt der Erfindung besteht darin, alle für die Gültigkeitsprüfung eines in einem Speicher eines Gerätes gespeicherten Gerätezertifikates erforderlichen Informationen ebenfalls in einem Speicher des Gerätes zu speichern, so dass jederzeit eine Identitätsprüfung des Gerätes ohne Einholen zusätzlicher Daten erfolgen kann, d.h. eine Offline-Prüfung des gespeicherten Gerätezertifikates ermöglicht wird.

15 Dementsprechend sieht ein Verfahren zum Erstellen von Gerätezertifikaten für elektronische Geräte vor, ein zu zertifizierendes elektronisches Gerät bereitzustellen, in welchem ein von außerhalb des Gerätes nicht auslesbares Geheimnis gespeichert ist, ein Gerätezertifikat für dieses
20 Gerät zu erzeugen, dessen Zertifikatsinformation kryptographisch an das in dem Gerät gespeicherte Geheimnis gebunden ist, wobei das Gerätezertifikat eine mit einem Signierschlüssel erzeugte digitale Signatur umfasst und mittels einer Zertifikatskette authentisierbar ist.

25

Die Zertifikatskette ist eine mit dem Gerätezertifikat beginnende Folge von wenigstens zwei Zertifikaten, wobei jedes Zertifikat der Zertifikatskette eine Information umfasst, welche den Gültigkeitszeitraum des jeweiligen
30 Zertifikates definiert, und wobei jedes Zertifikat der Zertifikatskette mit Ausnahme des Gerätezertifikates eine

Zertifikatsinformation umfasst, mit welcher das jeweils in der Folge vorhergehende Zertifikat authentisierbar ist.

Bei der Verwendung asymmetrischer Schlüsselpaare kann die
5 Echtheit der Signatur des Gerätezertifikates mit dem
öffentlichen Teil des Signierschlüssels des Ausstellers des
Gerätezertifikates geprüft werden. Für die Prüfung der
Authentizität des öffentlichen Teil des Signierschlüssels
des Ausstellers des Gerätezertifikates wird ein weiteres
10 digitales Zertifikat bereitgestellt. Für die Prüfung der
Authentizität des öffentlichen Teil des Signierschlüssels
des Ausstellers dieses weiteren digitalen Zertifikates kann
wiederum ein weiteres Zertifikates bereitgestellt werden.
Auf diese Weise wird die Zertifikatskette als Folge von
15 Zertifikaten aufgebaut, beginnend mit dem Gerätezertifikat,
die jeweils die Authentizität des öffentlichen Schlüssels
bestätigen, mit dem das vorhergehende Zertifikat geprüft
werden kann. Eine Zertifikatskette wird auch als
Validierungspfad oder Zertifizierungspfad bezeichnet.

20

Die Zertifikatskette umfasst das Gerätezertifikat und
wenigstens ein weiteres Zertifikat. Da auf das letzte
Zertifikat der Zertifikatskette kein weiteres Zertifikat
folgt, ist dies vorzugsweise ein vertrauenswürdiges
25 Zertifikat, bei welchem auf eine Prüfung der Echtheit
verzichtet werden kann.

Ferner sieht das Verfahren in einer ersten Variante vor,
für das erzeugte Gerätezertifikat eine
30 Bestätigungsinformation zu erstellen, welche bestätigt,
dass das Gerätezertifikat von einer autorisierten Instanz
erzeugt wurde. Das Bereitstellen der Zustandsinformationen

erfolgt dabei in der Regel mittels eines
Zertifikatsauskunftsdienstes.

Die Bestätigungsinformation kann beispielsweise darin
5 bestehen, dass das Gerätezertifikat oder eine aus dem
Gerätezertifikat abgeleitete Information abrufbar
gespeichert wird, zum Beispiel in einer Datenbank, welche
typischerweise von der die Gerätezertifikate ausstellenden
Instanz bereitgestellt wird.

10

Vorteilhaft kann das Verfahren auch das Bereitstellen einer
digital signierten Zustandsinformation für das
Gerätezertifikat umfassen, welche einen Nachweis umfasst,
dass das Gerätezertifikat von einer autorisierten Instanz
15 erzeugt wurde, wobei die Zustandsinformation unter
Ansprechen auf die Bestätigungsinformation bzw. nur bei
Vorliegen einer entsprechenden Bestätigungsinformation
erzeugt wird. Ferner kann auch vorteilhaft vorgesehen sein,
für wenigstens ein weiteres Zertifikat der Zertifikatskette
20 eine digital signierte Zustandsinformation bereitzustellen,
welche den Nachweis umfasst, dass das weitere Zertifikat
von einer autorisierten Instanz erzeugt wurde.

In einer zweiten Variante sieht das Verfahren ferner vor,
25 einen digital signierten Zeitstempel zu erzeugen, welcher
das Gerätezertifikat mit dem Zeitpunkt verknüpft, zu dem
der Zeitstempel erzeugt wird. Der digital signierte
Zeitstempel wird dabei vorzugsweise derart erzeugt, dass
das Gerätezertifikat oder ein Hash-Wert des
30 Gerätezertifikates zusammen mit der aktuellen Zeitangabe,
zum Beispiel in Form von Datum und Uhrzeit, mittels eines
Signierschlüssels digital signiert wird.

In einer besonders bevorzugten Ausführungsform des Verfahrens werden die beschriebene erste und zweite Variante kombiniert.

5

Vorzugsweise wird in der zweiten Variante des Verfahrens der digital signierte Zeitstempel von einem Server, welcher einen Zeitstempeldienst bereitstellt, in Antwort auf eine Anfrage zur Erstellung eines Zeitstempels erzeugt. Die
10 Anfrage wird beispielsweise von einem mit dem Server über ein Kommunikationsnetzwerk verbundenen Produktionscomputer zum Server und der erzeugte Zeitstempel zurück an den Produktionscomputer übertragen, wobei die Anfrage vorzugsweise das Gerätezertifikat oder einen Hash-Wert des
15 Gerätezertifikates umfasst.

Das erzeugte Gerätezertifikat und/oder wenigstens ein weiteres Zertifikat der Zertifikatskette und/oder der digital signierte Zeitstempel und/oder wenigstens eine
20 digital signierte Zustandsinformation werden vorzugsweise in einer dem Gerät zuordenbaren Weise abrufbar bereitgestellt. Dies kann beispielsweise durch Speichern in einem auslesbaren Speicher oder Speichermedium erfolgen, welches dem elektronischen Gerät zugeordnet oder im
25 elektronischen Gerät angeordnet ist. Beispielsweise kann als Speicher ein Flash-Speicher des Gerätes genutzt werden oder es wird dem Gerät ein Speichermedium wie zum Beispiel eine CD beigelegt. Alternativ können das erzeugte Gerätezertifikat und/oder wenigstens ein weiteres
30 Zertifikat der Zertifikatskette und/oder der digital signierte Zeitstempel und/oder wenigstens eine digital signierte Zustandsinformation beispielsweise über einen

Internet-Server zugänglich gemacht werden, welcher die Daten beispielsweise in Antwort auf eine Geräteidentifikation, wie zum Beispiel einer Seriennummer des Gerätes, bereitstellt. Dies kann beispielsweise durch
5 Einrichten eines entsprechenden Verzeichnisdienstes erfolgen.

Vorteilhaft werden die erzeugten Zeitstempel gezählt und der Server erzeugt und überträgt den Zeitstempel nur,
10 solange eine vorgegebene Obergrenze für die Anzahl der erzeugten Zeitstempel nicht überschritten wird. Zu diesem Zweck wird vorzugsweise an den Server, welcher den Zeitstempeldienst bereitstellt, ein Wert für diese Obergrenze übertragen und im Server gespeichert. Das Zählen
15 der Zeitstempel erfolgt beispielsweise derart, dass zunächst ein im Server gespeicherter Zähler auf Null gesetzt wird, der dann bei jeder Anfrage zur Erstellung eines Zeitstempels inkrementiert und mit dem gespeicherten Wert der Obergrenze verglichen wird. Ist der Zähler kleiner
20 oder gleich dem Wert der Obergrenze, so wird ein Zeitstempel erzeugt und zum Produktionscomputer übertragen, andernfalls wird kein Zeitstempel erzeugt, wobei in diesem Fall zum Produktionscomputer vorzugsweise eine entsprechende Fehlernachricht übertragen wird.

25 Auf diese Weise kann nur für eine vorgegebene begrenzte Anzahl von Geräten jeweils ein Gerätezertifikat mit zugeordnetem Zeitstempel erstellt werden. Dies ist besonders vorteilhaft zur Überwachung von
30 Produktionskontingenten bei Auftragsfertigung elektronischer Geräte.

Zur Erhöhung der Sicherheit werden vorzugsweise für die Erzeugung der digitalen Signatur des Gerätezertifikates und für die Erzeugung der digitalen Signatur des Zeitstempels unterschiedliche Signierschlüssel verwendet.

5

Ferner werden zur Erhöhung der Sicherheit vorzugsweise für die Erzeugung der digitalen Signatur des Gerätezertifikates und für die Erzeugung der digitalen Signatur der Zustandsinformationen unterschiedliche Signierschlüssel verwendet.

10

Wird eine unberechtigte Verwendung eines zum Signieren eines ersten Zertifikates der Zertifikatskette verwendeten Signierschlüssels erkannt, so wird vorteilhaft eine digital signierte Zustandsinformation für das in der Zertifikatskette auf das erste Zertifikat folgende Zertifikat erzeugt, wobei die Zustandsinformation eine Sperrinformation umfasst, welche das in der Zertifikatskette auf das erste Zertifikat folgende Zertifikat für Prüfzeitpunkte ab dem Zeitpunkt, zu dem die unberechtigte Verwendung erkannt wurde, als ungültig identifiziert.

15

20

In einer besonders vorteilhaften Ausführungsform des Verfahrens bildet das Geheimnis, welches kryptografisch an eine Zertifikatsinformation des Gerätezertifikates gebunden ist, den privaten Teil eines asymmetrischen Schlüsselpaares, wobei das Geheimnis vorzugsweise ein einmaliges Geheimnis ist. Somit ist vorzugsweise der private Schlüssel des Schlüsselpaares nicht auslesbar im Gerät gespeichert und der öffentliche Schlüssel des Schlüsselpaares ist Bestandteil der Zertifikatsinformation

25

30

des Gerätezertifikates, wobei das Gerät dazu ausgebildet ist, mittels des gespeicherten Geheimnisses eine Prüfung zu ermöglichen, ob eine Bindung des Gerätezertifikates an das Gerät besteht. Beispielsweise ist das Gerät dazu

5 ausgebildet, einen Wert zu empfangen, diesen mit dem gespeicherten privaten Schlüssel auf der Basis eines vorgegebenen Verschlüsselungsalgorithmus zu verschlüsseln und das Ergebnis in Antwort auf das Empfangen des Wertes auszugeben, so dass der ausgegebene Wert mit dem im

10 Gerätezertifikat enthaltenen öffentlichen Schlüssel entschlüsselt und mit dem ursprünglichen Wert verglichen werden kann, wobei bei Übereinstimmung eine Bindung des Gerätezertifikates an das Gerät besteht.

15 In einer bevorzugten Ausführungsform der Erfindung ist das Geheimnis in einem Chip des Gerätes gespeichert. Dieser Chip kann vorteilhaft als Chip gemäß der Spezifikation des Trusted Platform Module (TPM) der Trusted Computing Group, kurz TPM-Chip, ausgebildet sein, in welchem ein als PRIVEK

20 bezeichneter privater Schlüssel eines als "Endorsement Key" bezeichneten asymmetrischen Schlüsselpaars gespeichert ist. Auch kann ein solcher TPM-Chip selbst das elektronische Gerät bilden, für welches ein Gerätezertifikat erstellt wird. In diesem Fall kann

25 vorteilhaft zusätzlich ein weiteres Gerätezertifikat, zum Beispiel in Form eines Attributzertifikates, bereitgestellt werden, welches zur Bestätigung dient, dass ein bestimmter TPM-Chip im Gerät enthalten ist. Vorteilhaft kann das weitere Gerätezertifikat auf die gleiche Weise

30 bereitgestellt werden wie das Gerätezertifikat, d.h. beispielsweise im gleichen Speicher oder Speichermedium

gespeichert werden oder über den gleichen Verzeichnisdienst abrufbar bereitgestellt werden.

Ein Verfahren zur Prüfung der Gültigkeit eines nach dem
5 oben beschriebenen Verfahren erstellten Gerätezertifikates
sieht vor, ein Gerätezertifikat und ein vertrauenswürdiges
Zertifikat bereitzustellen, wobei das Gerätezertifikat mit
dem vertrauenswürdigen Zertifikat über eine
Zertifikatskette verkettbar ist, wobei die Zertifikatskette
10 eine mit dem Gerätezertifikat beginnende und mit dem
vertrauenswürdigen Zertifikat endende Folge von wenigstens
zwei Zertifikaten ist, wobei jedes Zertifikat der
Zertifikatskette eine Information umfasst, welche den
Gültigkeitszeitraum des jeweiligen Zertifikates definiert,
15 und wobei jedes Zertifikat der Zertifikatskette mit
Ausnahme des Gerätezertifikates eine Zertifikatsinformation
umfasst, mit welcher das jeweils in der Folge vorhergehende
Zertifikat authentisierbar ist, sowie einen zugeordneten
Prüfzeitpunkt für jedes Zertifikat der Zertifikatskette
20 festzulegen. Eine gültige Definition eines
Gültigkeitszeitraums kann insbesondere auch eine in die
Vergangenheit oder in die Zukunft gerichtete unbegrenzte
Gültigkeit umfassen, d.h. dass ein Ende oder beide Enden
des Gültigkeitszeitraumes unbegrenzt sind. Für diesen Zweck
25 können beispielsweise für den Anfang und/oder das Ende des
Gültigkeitszeitraumes jeweils Werte verwendet werden,
welche aufgrund einer vorgegebenen Konvention eine
unbegrenzte Gültigkeit repräsentieren.

30 Auf dieser Basis erfolgt eine erste Anzahl von Prüfungen,
und zwar eine Prüfung, ob das Gerätezertifikat mittels der
Zertifikatskette erfolgreich authentisierbar ist, ob für

jedes Zertifikat der Zertifikatskette der zugeordnete Prüfzeitpunkt innerhalb des Gültigkeitszeitraumes des jeweiligen Zertifikates liegt, und, mittels eines in einem Speicher des Gerätes hinterlegten Geheimnisses, ob eine
5 Bindung des Gerätezertifikates an das Gerät besteht.
Liefert die Prüfung in wenigstens einem Punkt ein negatives Ergebnis, so wird das Gerätezertifikat als ungültig erkannt.

10 Das beschriebene Verfahren zum Erstellen eines Gerätezertifikates für ein elektronisches Gerät und das beschriebene Verfahren zur Gültigkeitsprüfung eines so erstellten Gerätezertifikates bilden zusammen ein Verfahren zum Bestätigen der Identität eines elektronischen Gerätes
15 zum Zweck der Echtheits- oder Besitzprüfung. Insbesondere ermöglichen die erfindungsgemäßen Verfahren einen Schutz vor Fälschung eines Gerätezertifikates.

In einer ersten Variante des Prüfverfahrens wird für das
20 Gerätezertifikat eine zugeordnete, digital signierte Zustandsinformation bereitgestellt, wobei die Zustandsinformation das Gerätezertifikat als gültig oder ungültig identifiziert und eine Information umfasst, welche den Gültigkeitszeitraum der Zustandsinformation definiert.
25 In dieser Ausführungsvariante wird für die bereitgestellte Zustandsinformation zusätzlich geprüft, ob ein für die Zustandsinformation festgelegter Prüfzeitpunkt innerhalb des Gültigkeitszeitraumes der Zustandsinformation liegt und ob die Zustandsinformation das Gerätezertifikat als gültig
30 identifiziert, wobei die Kennzeichnung des Gerätezertifikates als gültig den Nachweis umfasst, dass das Gerätezertifikat von einer autorisierten Instanz

tatsächlich erzeugt wurde. Ist dieses Prüfergebnis positiv und auch die oben beschriebene erste Anzahl von Prüfungen erfolgreich, so wird das Gerätezertifikat als gültig erkannt, andernfalls als ungültig.

5

Vorteilhaft wird für wenigstens ein weiteres Zertifikat der Zertifikatskette eine zugeordnete, digital signierte Zustandsinformation bereitgestellt, wobei die Zustandsinformation das weitere Zertifikat als gültig oder ungültig identifiziert und eine Information umfasst, welche den Gültigkeitszeitraum der Zustandsinformation definiert. In dieser Ausführungsform wird für jede bereitgestellte Zustandsinformation geprüft, ob ein für die Zustandsinformation festgelegter Prüfzeitpunkt innerhalb des Gültigkeitszeitraumes der jeweiligen Zustandsinformation liegt und ob die Zustandsinformation das jeweils zugeordnete Zertifikat als gültig identifiziert, und das Gerätezertifikat nur bei positivem Prüfergebnis als gültig erkannt.

20

Die Zustandsinformationen können vorteilhaft zum Zweck der Gültigkeitsprüfung jeweils von einem Zertifikatsauskunftsdienst angefordert werden. Mit besonderem Vorteil umfasst eine bereitgestellte Zustandsinformation einen Positivnachweis der Existenz und Gültigkeit des jeweiligen Zertifikates, d.h. die Kennzeichnung des Zertifikates als gültig durch die Zustandsinformation umfasst vorteilhaft den Nachweis, dass das Zertifikat von einer autorisierten Instanz erzeugt wurde, wobei dieser Nachweis beispielsweise daraus abgeleitet sein kann, dass das Zertifikat oder eine aus dem Zertifikat abgeleitete Information in einer vorbestimmten

30

Datenbank gespeichert ist. Zur Prüfung, ob ein Zertifikat oder eine aus einem Zertifikat abgeleitete Information in einer vorbestimmten Datenbank gespeichert ist, kann der Server, welcher den Zertifikatsauskunftsdiens
5 bereitstellt, vorzugsweise mit der Datenbank über ein Kommunikationsnetzwerk kommunizieren.

Mit besonderem Vorteil sieht das Verfahren zur Gültigkeitsprüfung ein spezielles Gültigkeitsmodell vor,
10 wobei die Prüfzeitpunkte für die Zertifikate der Zertifikatskette und/oder für die zugeordneten Zustandsinformationen auf bestimmte Weise festgelegt werden.

15 Im einfachsten Fall kann als zugeordneter Prüfzeitpunkt für wenigstens eines der Zertifikate der Zertifikatskette und/oder wenigstens eine der Zustandsinformationen der Zeitpunkt festgelegt werden, zu dem die Prüfung der Gültigkeit des Gerätezertifikates durchgeführt wird.

20

In einer zweiten Variante des Prüfverfahren ist vorgesehen, einen dem Gerätezertifikat zugeordneten digital signierten Zeitstempel bereitzustellen, welcher das Gerätezertifikat mit einem Zeitpunkt verknüpft, wobei als zugeordneter
25 Prüfzeitpunkt für wenigstens eines der Zertifikate der Zertifikatskette der über den Zeitstempel mit dem Gerätezertifikat verknüpfte Zeitpunkt festgelegt wird.

In dieser zweiten Ausführungsvariante wird zusätzlich
30 geprüft, ob der Zeitstempel erfolgreich authentisierbar ist. Ist dies der Fall und auch die oben beschriebene erste Anzahl von Prüfungen wird erfolgreich durchgeführt, so wird

das Gerätezertifikat als gültig erkannt, andernfalls als ungültig.

Auch in dieser zweiten Ausführungsvariante kann vorteilhaft
5 für wenigstens ein Zertifikat der Zertifikatskette eine
zugeordnete, digital signierte Zustandsinformation
bereitgestellt werden, wobei die Zustandsinformation das
Zertifikat als gültig oder ungültig identifiziert und eine
Information umfasst, welche den Gültigkeitszeitraum der
10 Zustandsinformation definiert. Wie oben bereits für die
erste Ausführungsvariante beschrieben, wird in dieser
Ausführungsform für jede bereitgestellte
Zustandsinformation geprüft, ob ein für die
Zustandsinformation festgelegter Prüfzeitpunkt innerhalb
15 des Gültigkeitszeitraumes der jeweiligen
Zustandsinformation liegt und ob die Zustandsinformation
das jeweils zugeordnete Zertifikat als gültig
identifiziert, und das Gerätezertifikat nur bei positivem
Prüfergebnis als gültig erkannt. Auch in dieser
20 Ausführungsvariante umfasst eine bereitgestellte
Zustandsinformation vorzugsweise einen Positivnachweis der
Existenz und Gültigkeit des jeweiligen Zertifikates.

Besonders vorteilhaft kann auch als zugeordneter
25 Prüfzeitpunkt für wenigstens eine der Zustandinformationen
der über den digital signierten Zeitstempel mit dem
Gerätezertifikat verknüpfte Zeitpunkt festgelegt werden.

In einer besonders vorteilhaften Ausführungsform des
30 Verfahrens wird als zugeordneter Prüfzeitpunkt für das
Gerätezertifikat der Zeitpunkt festgelegt, zu dem die
Prüfung der Gültigkeit des Gerätezertifikates durchgeführt

wird, und für alle weiteren Zertifikate der Zertifikatskette wird der über den authentisierten Zeitstempel mit dem Gerätezertifikat verknüpfte Zeitpunkt festgelegt. Insbesondere wird der Zeitpunkt der Prüfung nur
5 mit dem Gültigkeitszeitraum des Gerätezertifikates verglichen, während für alle anderen Gültigkeitskriterien auch des Gerätezertifikates die Zeitangabe aus dem Zeitstempel verwendet wird, d.h. dass in dieser Ausführungsform insbesondere keine Sperrinformation für das
10 Gerätezertifikat betrachtet wird.

Ferner kann vorteilhaft vorgesehen sein, dass als zugeordneter Prüfzeitpunkt für wenigstens eines der Zertifikate der Zertifikatskette und/oder für die diesem
15 Zertifikat zugeordnete Zustandsinformation der Zeitpunkt festgelegt wird, zu dem das in der Zertifikatskette vorhergehende Zertifikat erstellt wurde oder zu dem der Gültigkeitszeitraum des in der Zertifikatskette vorhergehenden Zertifikates beginnt.

20

Für das bei der Gültigkeitsprüfung eingesetzte Gültigkeitsmodell kann auch eine Kombination der oben beschriebenen Varianten vorgesehen sein.

25 Mit besonderem Vorteil ist das Gültigkeitsmodell derart ausgestaltet, dass alle zur Gültigkeitsprüfung des Gerätezertifikates benötigten Informationen zum Zeitpunkt der Erstellung des Gerätezertifikates eingeholt werden können. Diese Informationen umfassen insbesondere alle
30 Zertifikate der zur Authentisierung des Gerätezertifikates eingesetzten Zertifikatskette, jeweils zugeordnete Zustandsinformationen, sowie gegebenenfalls erforderliche

Nachweise zur Prüfung der Gültigkeit der Zustandsinformationen. Bei Einsatz eines Zeitstempels umfassen die Informationen insbesondere auch alle Auskünfte und Nachweise, die zur Authentisierung des Zeitstempels selbst erforderlich sind.

Je nach Einsatzzweck kann das Gerätezertifikat die Funktion eines Echtheitszertifikates oder Besitzzertifikates aufweisen und/oder in Form eines Attributzertifikates ausgebildet sein, wobei ein Echtheitszertifikat typischerweise vom Gerätehersteller ausgestellt wird, um einem Gerätebesitzer die Prüfung der Echtheit eines Gerätes zu ermöglichen, ein Besitzzertifikat zur Besitzkennzeichnung vom Gerätebesitzer selbst ausgestellt wird, und ein Attributzertifikat zur Bestätigung einer bestimmten Eigenschaft eines Gerätes dient, beispielsweise zur Bestätigung, dass in einem Gerät ein bestimmtes Modul, zum Beispiel ein TPM-Chip, integriert ist.

Vorzugsweise umfasst die Zertifikatskette wenigstens ein Zwischenzertifikat, welches in der durch die Zertifikatskette definierten Reihenfolge zwischen dem Gerätezertifikat und dem vertrauenswürdigen Zertifikat angeordnet ist, wobei das vertrauenswürdige Zertifikat vorzugsweise ein selbstsigniertes Wurzelzertifikat ist. Das Zwischenzertifikat dient insbesondere der Authentisierung eines vom Gerätehersteller zum Signieren von Gerätezertifikaten eingesetzten Signierschlüssels, nachfolgend als Manufacturer's Attestation Key (MAKey) bezeichnet. Die eingesetzten MAKeys können auch in mehreren Hierarchieebenen strukturiert sein, wobei die Zertifikatskette dann mehrere Zwischenzertifikate umfasst.

Es kann auch ganz auf Zwischenzertifikate verzichtet werden, beispielsweise wenn die Gerätezertifikate direkt mit einem Wurzelschlüssel signiert werden.

- 5 Das oben genannte technische Problem wird ferner durch ein System zum Erstellen von Gerätezertifikaten für elektronische Geräte gelöst, wobei das System dazu ausgebildet ist, das oben beschriebene Verfahren zum Erstellen von Gerätezertifikaten für elektronische Geräte
- 10 auszuführen. Dementsprechend umfasst das System einen Produktionscomputer mit einem darin gespeicherten Signierschlüssel zum Erzeugen von Gerätezertifikaten für elektronische Geräte, wobei der Produktionscomputer dazu ausgebildet ist, auf einen Speicher des jeweiligen
- 15 elektronischen Gerätes zuzugreifen. Zu diesem Zweck ist der Produktionscomputer mit wenigstens einem elektronischen Gerät verbindbar, vorzugsweise über ein Kommunikationsnetzwerk.
- 20 Ferner umfasst das System in einer ersten Variante eine mit dem Produktionscomputer verbindbare Datenbank, in welcher der Produktionscomputer erzeugte Gerätezertifikate oder daraus abgeleitete Werte speichert, wobei die Datenbank dazu ausgebildet ist, auf Anfrage eine Information
- 25 bereitzustellen, ob ein angefragtes Gerätezertifikat oder ein aus einem angefragten Gerätezertifikat abgeleiteter Wert in der Datenbank gespeichert ist.

In einer zweiten Variante umfasst das System einen mit dem

30 Produktionscomputer verbindbaren Server, welcher einen Zeitstempeldienst bereitstellt, und welcher auf Anfrage des Produktionscomputers für ein vom Produktionscomputer

vorgegebenes Gerätezertifikat einen digital signierten Zeitstempel erzeugt und zum Produktionscomputer überträgt, wobei der Zeitstempel das vorgegebene Gerätezertifikat mit dem Zeitpunkt verknüpft, zu dem der Zeitstempel erzeugt wird.

In einer besonders bevorzugten Ausführungsform umfasst das System die Merkmale beider oben beschriebenen Varianten.

Das System kann ferner vorteilhaft dazu ausgebildet sein, jede der oben beschriebenen Ausführungsformen des Verfahrens zum Erstellen von Gerätezertifikaten für elektronische Geräte auszuführen und kann zu diesem Zweck weitere geeignete Komponenten umfassen.

Das oben genannte technische Problem wird ferner durch ein Prüfsystem zur Prüfung der Gültigkeit eines Gerätezertifikates gelöst, wobei das Prüfsystem zum Durchführen des oben beschriebenen Verfahrens zur Gültigkeitsprüfung ausgebildet ist. Dementsprechend umfasst das Prüfsystem ein Prüfgerät zum Prüfen der Gültigkeit eines in einem Speicher eines elektronischen Gerätes hinterlegten Gerätezertifikates mittels einer Zertifikatskette, sowie einen Zertifikatsauskunfts-Server, auf welchen das Prüfgerät zugreifen kann, um Zustandsinformationen für wenigstens ein Zertifikat der Zertifikatskette abzufragen. Das Prüfgerät umfasst zu diesem Zweck vorteilhaft eine entsprechende Prüf-Applikation in Form einer Software.

Das Prüfsystem kann ferner vorteilhaft dazu ausgebildet sein, jede der oben beschriebenen Ausführungsformen des

Verfahrens zur Gültigkeitsprüfung eines Gerätezertifikates auszuführen und kann zu diesem Zweck weitere geeignete Komponenten umfassen. So kann das Prüfsystem beispielsweise ferner eine Datenbank oder einen Datenbankauszug umfassen, auf welchen der Zertifikatsauskunfts-Server zum Erzeugen von Zustandsinformationen zugreifen kann, welche Positivnachweise umfassen.

Das oben genannte technische Problem wird auch durch ein elektronisches Gerät gelöst, welches einen von außerhalb des Gerätes nicht auslesbaren Speicher mit einem darin gespeicherten Geheimnis, sowie einen auslesbaren Speicher umfasst, wobei in dem auslesbaren Speicher die für die Durchführung des oben beschriebenen Verfahrens zur Gültigkeitsprüfung eines Gerätezertifikates erforderlichen Informationen gespeichert sind, insbesondere das Gerätezertifikat, alle weiteren für die Gültigkeitsprüfung des Gerätezertifikates erforderlichen Zertifikate der Zertifikatskette, sowie Zustandsinformationen und/oder Zeitstempel. Die gespeicherten Informationen sind dabei jeweils in Abhängigkeit der für die jeweilige Ausführungsform des Verfahrens zur Gültigkeitsprüfung erforderlichen Informationen ausgewählt.

Sind in dem elektronischen Gerät alle zum Durchführen einer Prüfung der Gültigkeit eines im Gerät gespeicherten Gerätezertifikates gespeichert, so kann eine Gültigkeitsprüfung mit besonderem Vorteil offline erfolgen, d.h. ohne Zugriff auf weitere Informationsquellen. Insbesondere kann auch auf einen Zugriff auf einen Zertifikatsauskunfts-Server verzichtet werden, so dass ein

Prüfsystem in diesem Fall besonders vorteilhaft nur das Prüfgerät und das zu prüfende elektronische Gerät umfasst.

Es ist typischerweise nicht erforderlich, das
5 beispielsweise als selbstsigniertes Wurzelzertifikat ausgebildete vertrauenswürdige Zertifikat im Gerät zu speichern, da das Prüfgerät dieses Zertifikat typischerweise selbst kennt.

10 Mit besonderem Vorteil kann ferner das Prüfgerät durch das zu prüfende Gerät selbst gebildet sein, d.h. das zu prüfende Gerät kann dazu ausgebildet sein, selbst die Gültigkeitsprüfung des gespeicherten Gerätezertifikates durchzuführen und kann dementsprechend zu diesem Zweck eine
15 entsprechende Prüf-Applikation aufweisen.

Auch können die für die Durchführung des oben beschriebenen Verfahrens zur Gültigkeitsprüfung eines Gerätezertifikates erforderlichen Informationen vollständig oder teilweise
20 statt in einem Speicher des Gerätes in einem dem Gerät zugeordneten Speicher gespeichert werden.

Dementsprechend wird das oben genannte technische Problem auch durch ein Speichermedium gelöst, welches einem
25 elektronischen Gerät zugeordnet ist, wobei das elektronische Gerät einen von außerhalb des Gerätes nicht auslesbaren Speicher mit einem darin gespeicherten Geheimnis umfasst, und wobei in dem Speichermedium alle für die Durchführung des oben beschriebenen Verfahrens zur
30 Gültigkeitsprüfung eines Gerätezertifikates erforderlichen Informationen, insbesondere das Gerätezertifikat, alle weiteren für die Gültigkeitsprüfung des Gerätezertifikates

erforderlichen Zertifikate der Zertifikatskette, sowie Zustandsinformationen und/oder Zeitstempel, gespeichert sind.

- 5 Das Speichermedium kann beispielsweise als eine dem Gerät beigelegte CD ausgebildet sein. Es liegt aber auch jede andere geeignete Form eines Speichermediums im Rahmen der Erfindung. Die Zuordnung des Speichermediums zu dem elektronischen Gerät kann allein durch ein gemeinsames
- 10 Bereitstellen als Set erfolgen. Das Speichermedium kann aber beispielsweise auch entsprechend gekennzeichnet werden, zum Beispiel durch Speichern oder Aufdrucken einer Seriennummer des Gerätes auf dem Speichermedium.
- 15 Durch die Erfindung werden auf besonders einfache Weise Zertifikate automatisch als Fälschung erkannt, die unter unautorisierter Verwendung der zugehörigen Signierschlüssel erzeugt wurden.
- 20 Die Erfindung wird nachfolgend beispielhaft anhand bevorzugter Ausführungsformen und unter Bezugnahme auf die beigefügten Zeichnungen genauer beschrieben. Dabei bezeichnen gleiche Bezugszeichen in den Zeichnungen gleiche oder ähnliche Teile. Es zeigen:
- 25
- Fig. 1 eine schematische Darstellung eines beispielhaften Systems zum Erstellen von Gerätezertifikaten für elektronische Geräte,
- Fig. 2 schematisch eine zur Gültigkeitsprüfung eines Gerätezertifikates eingesetzten Zertifikatskette,
- 30 Fig. 3 eine schematische Darstellung eines beispielhaften Prüfsystems, ausgebildet zur

Prüfung der Bindung eines Gerätezertifikates an
ein elektronisches Gerät,

Fig. 4 schematisch zwei getrennte Zertifikatsketten zur
Gültigkeitsprüfung bei Verwendung eines
Attributzertifikates zu einem Gerätezertifikat,

Fig. 5a eine schematische Darstellung einer ersten
bevorzugten Ausführungsform eines Systems zum
Erstellen von Gerätezertifikaten,

Fig. 5b schematisch ein zur Gültigkeitsprüfung von mit
einem in Fig. 5a dargestellten System erstellten
Gerätezertifikaten ausgebildetes Prüfsystem,

Fig. 6a eine schematische Darstellung einer zweiten
bevorzugten Ausführungsform eines Systems zum
Erstellen von Gerätezertifikaten,

Fig. 6b schematisch ein zur Gültigkeitsprüfung von mit
einem in Fig. 6a dargestellten System erstellten
Gerätezertifikaten ausgebildetes Prüfsystem,

Fig. 7a eine schematische Darstellung einer dritten
bevorzugten Ausführungsform eines Systems zum
Erstellen von Gerätezertifikaten,

Fig. 7b schematisch ein zur Gültigkeitsprüfung von mit
einem in Fig. 7a dargestellten System erstellten
Gerätezertifikaten ausgebildetes Prüfsystem,

Fig. 8 eine schematische Darstellung der
Gültigkeitszeiträume von Zertifikaten und
Zustandsinformationen bei Verwendung eines ersten
bevorzugten Gültigkeitsmodells,

Fig. 9 eine schematische Darstellung der
Gültigkeitszeiträume von Zertifikaten und
Zustandsinformationen bei Verwendung eines
zweiten bevorzugten Gültigkeitsmodells,

- Fig. 10 eine schematische Darstellung der
Gültigkeitszeiträume von Zertifikaten und
Zustandsinformationen bei Verwendung eines
dritten bevorzugten Gültigkeitsmodells,
5 Fig. 11a eine schematische Darstellung einer vierten
bevorzugten Ausführungsform eines Systems zum
Erstellen von Gerätezertifikaten, und
Fig. 11b schematisch ein zur Gültigkeitsprüfung von mit
einem in Fig. 11a dargestellten System erstellten
10 Gerätezertifikaten ausgebildetes Prüfsystem.

Bei den nachfolgend beschriebenen Ausführungsformen der
Erfindung wird davon ausgegangen, dass ein Chiphersteller
Trusted Platform Module (TPMs), im Folgenden auch als TPM-
15 Chip oder kurz als TPM bezeichnet, herstellt und vertreibt,
welche von ihm jeweils mit einem einmaligen Schlüsselpaar
ausgestellt sind, dem sogenannten Endorsement Key (EK)
bestehend aus privatem (PRIVEK) und öffentlichem Teil
(PUBEK). Der PRIVEK wird im TPM generiert und gespeichert,
20 ohne es je zu verlassen.

Der Gerätehersteller integriert ein TPM in sein Gerät.
Dabei erstellt er mit einer eigenen Zertifizierungsstelle
(Certification Authority, CA) ein elektronisch signiertes
25 Zertifikat (Endorsement Certificate, EK-Zertifikat) in Form
eines Public-Key-Zertifikates, welches den öffentlichen
Teil (PUBEK) des Endorsement-Keys digital signiert.

Die Signatur des EK-Zertifikates entsteht unter Verwendung
30 eines privaten Schlüssels, welcher nur dem Gerätehersteller
zur Verfügung steht. Dieser private Schlüssel wird im
Folgenden als Manufacturer's Attestation Key (MAKey)

bezeichnet. Die dem Gerätehersteller eigene
Zertifizierungsstelle wird vor dem Erzeugen des EK-
Zertifikats dazu genutzt, um den zum MAKey gehörenden
öffentlichen Schlüssel ebenfalls mittels Public-Key-
5 Zertifikat als zum Gerätehersteller gehörend zu bestätigen.
Das zum MAKey gehörende Zertifikat wird folgend mit MACert
bezeichnet. Es wird im Range eines sogenannten
Zwischenzertifikates einer Zertifizierungsstelle verwendet
(intermediate CA certificate, Sub-CA-Zertifikat).
10 Gegebenenfalls verwendet der Gerätehersteller mehrere
private Schlüssel bei der Herstellung, beispielsweise
MAKey1, MAKey2, MAKey3 und so weiter. Zu jedem privaten
Schlüssel existiert ein entsprechendes Zertifikat, MACert1,
MACert2, MACert3 und so weiter. Alle diese Zertifikate sind
15 direkt oder indirekt durch die Zertifizierungsstelle des
Herstellers bestätigt, zum Beispiel indem der
Wurzelschlüssel der Zertifizierungsstelle, im Folgenden als
Manufacturer's Trust Anchor Key, kurz MTAKey, bezeichnet,
verwendet wurde, um sie digital zu signieren. Der
20 Wurzelschlüssel wird mit Hilfe eines selbst-signierten
Wurzelzertifikates (fortan Manufacturer's Trust Anchor
Certificate, kurz MTACert) bestätigt und vom Hersteller
veröffentlicht.

25 Zu diesem Vorgang ist die Infrastruktur eines
Geräteherstellers beispielhaft in Fig. 1 dargestellt. An
einem Produktionsarbeitsplatz 200 ist der Schlüssel MAKey1
und das Zertifikat MACert1 im Einsatz, wobei diese in einem
Speicher 210 gespeichert sind. Das Zertifikat wurde von
30 einer in Fig. 1 nicht dargestellten, privaten
Zertifizierungsstelle ausgestellt, die nun abgeschaltet
ist. Am Produktionsarbeitsplatz 200 werden beispielhaft die

Geräte 101, 102 und 103 initialisiert, welche bereits zusammengebaut sind und jeweils ein TPM 111, 112 bzw. 113 enthalten, welches wiederum jeweils einen individuellen EK enthält. Zu dem PUBEK eines TPM wird am

5 Produktionsarbeitsplatz 200 mit Hilfe einer Software-Anwendung ein Gerätezertifikat (EKCert1, EKCert2, ...) erzeugt, indem es mit MAKey1 unterschrieben wird. Das Gerätezertifikat wird im dargestellten Ausführungsbeispiel zusammen mit dem MACert1 in persistentem Speicher des

10 Gerätes 101, 102 bzw. 103 abgelegt. Zu diesem Zweck ist der Produktionsarbeitsplatz 200 mit den Geräten 101, 102 und 103 über ein Kommunikationsnetzwerk verbunden, wobei vorzugsweise eine Vielzahl von Geräten gleichzeitig an das Kommunikationsnetzwerk angeschlossen sein können.

15 Alternativ zur Speicherung des Gerätezertifikates und des Zertifikates MACert1 in einem Speicher des Gerätes 101, 102 bzw. 103 können diese Daten auch auf einem Speichermedium wie beispielsweise einer Compact Disc (CD) gespeichert werden, welche dem Gerät zuordenbar ist, beispielsweise dem

20 Gerät beiliegt. Da prinzipiell nur erforderlich ist, dass die Daten in einer dem Gerät zuordenbaren Weise abrufbar bereitgestellt werden, könne die Daten beispielsweise auch mittels eines Verzeichnisdienstes bereitgestellt werden, von welchem sie bei Bedarf abgerufen werden können. Es kann

25 aber auch jede andere geeignete Weise der Bereitstellung eingesetzt werden.

In dem dargestellten Beispiel werden die erzeugten Gerätezertifikate ferner in einer Herstellerdatenbank 300

30 gespeichert, auf welche vom Produktionsarbeitsplatz 200 zugegriffen werden kann. Die Verbindung zwischen Produktionsarbeitsplatz 200 und Herstellerdatenbank 300

kann dabei über das gleiche oder ein anderes Kommunikationsnetzwerk oder auch über eine Direktverbindung erfolgen.

5 Später verwendet ein Gerätebesitzer zum Beispiel nach dem Erwerb eines Gerätes den vom Hersteller veröffentlichten Wurzelschlüssel aus dem Wurzelzertifikat (MTACert), um die Echtheit des Gerätes elektronisch zu prüfen. Ein gängiges Verfahren ist beispielsweise, dass der Gerätebesitzer ein
10 Software-Werkzeug verwendet, welches das MTACert kennt und über Kommunikationswege mit dem Gerät von diesem das entsprechende EK-Zertifikat (EKCert1, EKCert2, ...) sowie alle relevanten Zwischenzertifikate, beispielsweise MACert1, erhält. Das Software-Werkzeug prüft dann den
15 Zertifizierungspfad, im Folgenden auch als Zertifikatskette bezeichnet, vom Gerätezertifikat (EK-Zertifikat) bis zum Wurzelzertifikat (MTACert) durch Validierung dieses Pfades, insbesondere gemäß RFC 5280. Damit ist lediglich die Echtheit des EK-Zertifikates bestimmt, eingeschränkt unter
20 der Voraussetzung, dass bis zum Zeitpunkt der Prüfung keiner der vom Hersteller verwendeten privaten Schlüssel (MTAKey und MAKey1, MAKey2, MAKey3, ...) unautorisiert verwendet wurde.

25 Ein Beispiel für den Zertifizierungspfad ist in Fig. 2 dargestellt. Dementsprechend umfasst die Zertifikatskette das als EKCert1 bezeichnete Gerätezertifikat 630, das als MACert1 bezeichnete Zwischenzertifikat 620 und das als MTACert bezeichnete Wurzelzertifikat 610.

30

Das Gerätezertifikat 630 umfasst die Zertifikatsinformation 530 und die Signatur 430, welche durch einen Signiervorgang

400 erzeugt wird, bei welchem die Zertifikatsinformation
530 mit dem als MAKey1_PRIV bezeichneten privaten Schlüssel
525 verschlüsselt wird. Der Signiervorgang 400 kann
alternativ vorsehen, dass nicht die Zertifikatsinformation
5 530 digital signiert wird, sondern eine aus der
Zertifikatsinformation 530 gebildete kryptographische
Prüfsumme, wie zum Beispiel ein Hashwert der
Zertifikatsinformation 530, mit dem als MAKey1_PRIV
bezeichneten privaten Schlüssel 525 verschlüsselt wird.

10

Die Zertifikatsinformation 530 des Gerätezertifikates 630
umfasst den öffentlichen Schlüssel EK1_PUB. Zusätzlich kann
die Zertifikatsinformation 530 weitere Informationen
umfassen, wie zum Beispiel Informationen zur
15 Gültigkeitsdauer des Gerätezertifikates 630, eine
Identifikationsinformation des Zertifikatsausstellers,
Informationen zum Eigentümer des öffentlichen Schlüssels
EK1_PUB, Informationen zu Regeln und Verfahren, unter denen
das Gerätezertifikat 630 ausgegeben wurde und/oder Angaben
20 zum zulässigen Anwendungs- und Geltungsbereich des
öffentlichen Schlüssels EK1_PUB.

25

Das Zwischenzertifikat 620 umfasst die
Zertifikatsinformation 520 und die Signatur 420, welche
durch einen Signiervorgang 400 erzeugt wird, bei welchem
die Zertifikatsinformation 520 oder eine aus der
Zertifikatsinformation 520 gebildete kryptographische
Prüfsumme mit dem als MTAKey_PRIV bezeichneten privaten
Schlüssel 515 verschlüsselt wird. Die

30

Zertifikatsinformation 520 des Zwischenzertifikates 620
umfasst zumindest den öffentlichen Schlüssel MAKey1_PUB,
sowie gegebenenfalls weitere Informationen analog zu den

oben bezüglich der Zertifikatsinformation 530 beschriebenen Informationen.

Das Wurzelzertifikat 610 umfasst die Zertifikatsinformation
5 510 und die digitale Signatur 410. Das Wurzelzertifikat 610
ist selbstsigniert, d.h. die digitale Signatur wird durch
einen Signiervorgang 400 erzeugt, bei welchem die
Zertifikatsinformation 510 oder eine aus der
Zertifikatsinformation 510 gebildete kryptographische
10 Prüfsumme mit MTAKey_PRIV verschlüsselt wird. Die
Zertifikatsinformation 510 des Wurzelzertifikates 610
umfasst zumindest den öffentlichen Schlüssel MTAKey_PUB,
sowie analog zu den oben beschriebenen
Zertifikatsinformationen 530 und 520 gegebenenfalls weitere
15 Informationen.

Wie in Fig. 3 dargestellt, stellt das Software-Werkzeug in
einem nächsten Schritt sicher, dass das EK-Zertifikat
EKCert1 auch wirklich zum vorliegenden Gerät 101 gehört.
20 Hierzu können verschiedene Verfahren eingesetzt werden.
Beispielsweise fordert das beispielsweise in einem
Prüfcomputer 700 installierte Software-Werkzeug das Gerät
101 über einen Kommunikationskanal auf, eine vom Software-
Werkzeug generierte Zufallszahl z mit Hilfe des im TPM 111
25 gespeicherten privaten Schlüssels PRIVEK, im dargestellten
Beispiel als EK1_PRIV bezeichnet, zu signieren. Technisch
bedeutet dies eine Verschlüsselung der Zufallszahl z bzw.
eines in Abhängigkeit von z gebildeten Wertes mittels
PRIVEK. Der in Abhängigkeit der Zufallszahl z gebildete
30 Wert kann beispielsweise eine kryptographische Prüfsumme
von z oder eine kryptographische Prüfsumme von z und
weiteren Informationen sein, wobei die kryptographische

Prüfsumme beispielsweise ein Hashwert ist, und wobei die zusätzlichen Informationen geräteseitig bekannt und gegebenenfalls auch öffentlich bekannt sein können. Sobald das Gerät 101 die Signatur S zurück übermittelt, prüft das Software-Werkzeug die Signatur, indem es mittels des im dargestellten Beispiel als EK1_PUB bezeichneten öffentlichen Schlüssels PUBEK, welcher im EK-Zertifikat EKCert1 enthalten ist, die Zufallszahl z bzw. die aus z gebildete kryptographische Prüfsumme aus der Signatur S entschlüsselt und mit der ursprünglichen Zufallszahl z bzw. mit einer in Abhängigkeit der ursprünglichen Zufallszahl z gebildeten kryptographischen Prüfsumme vergleicht. Zu diesem Zweck werden im dargestellten Ausführungsbeispiel zusammen mit der Signatur S die im Speicher 121 gespeicherten Zertifikate EKCert1 und MACert1 vom Gerät 101 zum Prüfcomputer 700 übertragen. Das Zertifikat MTACert ist typischerweise bereits in einem Speicher 710 des Prüfcomputers 700 gespeichert.

Gemäß Spezifikation des TPM-Chips ist der PRIVEK nicht aus dem TPM 111 extrahierbar und global einmalig. Demnach ist mit dem beschriebenen Verfahren die Echtheit des Gerätes 101 bestimmt unter den bereits genannten Einschränkungen und sofern der TPM-Chip 111 nicht aus dem Gerät 101 entfernt und in ein anderes Gerät integriert wurde.

Hersteller von TPM-Chips erstellen häufig bereits bei der Produktion der Chips jeweils ein EK-Zertifikat. In diesem Fall werden also EK und EK-Zertifikat beim Hersteller des TPM-Chips erzeugt. Der Unterschied zu dem oben beschriebenen Fall besteht darin, dass an zwei Stellen eine Zertifizierungsstelle (CA) benötigt wird, um die Echtheit

zu bestätigen. Eine Zertifizierungsstelle wird beim Hersteller von TPM-Chips und ein anderes Mal beim Hersteller von Geräten benötigt. Weiter kann beim Gerätehersteller auf das Ausstellen eines Public-Key-Zertifikates verzichtet werden. Der Gerätehersteller stellt stattdessen ein Attributzertifikat zum bestehenden EK-Zertifikat aus, mit dem er bestätigt, dass ein bestimmtes TPM in einem bestimmten Gerät verbaut wurde. Das Attributzertifikat wird als Plattform-EK-Zertifikat bezeichnet.

Der Mehrwert für den späteren Gerätebesitzer besteht darin, dass separat die Echtheit des TPM-Chips als auch die Echtheit des Gerätes überprüft werden kann. Dabei werden zwei Wurzelzertifikate benötigt und zwei Zertifikatsketten geprüft aber nur eine Signatur verifiziert. Die beiden Zertifikatsketten sind in Fig. 4 dargestellt. Dort existiert die Verbindung zwischen dem Plattform-EK-Zertifikat ohne öffentlichen Teil EK1_PUB von EK1 und dem EKCert1 mit öffentlichem Teil EK1_PUB von EK1 aufgrund einer Referenz, zum Beispiel in Form einer Zertifikatsnummer zusammen mit einem kryptographischen Hash-Wert, der über den Inhalt von EKCert1 berechnet und im Plattform-EK-Zertifikat enthalten ist. Die auf der linken Seite der Fig. 4 dargestellte Zertifikatskette zur Authentisierung des vom TPM-Hersteller erzeugten EK-Zertifikates EKCert1 entspricht der in Fig. 2 dargestellten Zertifikatskette. Der mittels einer Hash-Funktion 450 aus EKCert1 erzeugte Hash-Wert 530' bildet die Zertifikatsinformation des Plattform-EK-Zertifikates 630', welches ferner die Signatur 430' umfasst. Das Plattform-EK-Zertifikates 630', sowie die weiteren Zertifikate 620' und

610\, umfassend die Zertifikatsinformationen 520\ bzw. 510\ und die Signaturen 420\ bzw. 410\, werden analog zu der in Fig. 2 dargestellten Zertifikatskette gebildet.

5 Bestimmte Geräte können private Schlüssel auch ohne TPM-Chip sicher verwahren. In solchen Fällen aber auch bei Geräten mit TPM besteht die Möglichkeit, dass während der Herstellung der Geräte jeweils ein neues Geheimnis erzeugt und durch den Hersteller mit einem Gerätezertifikat
10 versehen wird. Zum Beispiel kann anstelle des oder zusätzlich zum Endorsement-Key (EK) ein neues asymmetrisches Schlüsselpaar erzeugt werden und der öffentliche Schlüssel durch ein Zertifikat des Herstellers wie oben beschrieben bestätigt werden. Wenn ein TPM
15 vorhanden ist, kann dieses neue Schlüsselpaar auch kryptographisch an das TPM gebunden werden. In beiden Fällen besteht eine Zertifikatskette wie oben beschrieben. Der Hersteller stellt ein Public-Key-Zertifikat aus. In dieser Variante ist es aber unabhängig von einem
20 öffentlichen Schlüssel, der anderswo erzeugt wurde. Insbesondere hat es keine Verbindung zu einem öffentlichen Teil eines EK, der von einem TPM-Hersteller erzeugt wurde. Die Unabhängigkeit mag als Vorteil angesehen werden. Jedoch ist der Gerätehersteller dann für die Einmaligkeit des
25 Schlüsselpaares verantwortlich.

Die relevanten Gültigkeitszeiträume bei Einsatz eines PKIX-Verfahrens sind beispielhaft in Fig. 8 dargestellt. Üblicherweise haben die Wurzelzertifikate einen sehr langen
30 Gültigkeitszeitraum 810 von mehreren Jahren. Für das PKIX-Verfahren umfasst der Gültigkeitszeitraum von Wurzelzertifikaten denjenigen aller abhängigen Zertifikate.

So umfasst die in Fig. 8 dargestellte Gültigkeitsdauer 810 für das Zertifikat MTACert auch diejenigen für die Zertifikate MACert1 und EKCert1, welche für MACert1 mit Bezugszeichen 820 und für EKCert1 mit Bezugszeichen 830 bezeichnet sind. Für Sub-CA-Zertifikate gilt ebenfalls, dass ihr Gültigkeitszeitraum denjenigen aller abhängigen Zertifikate umfasst. In Fig. 8 umfasst dementsprechend die Gültigkeit von MACert1 jene von EKCert1.

Sobald eine Zertifikatskette bestehend aus MTACert, MACert1 und EKCert1 zu einem Zeitpunkt t_0 auf Gültigkeit überprüft wird muss nach PKIX der Zeitpunkt t_0 innerhalb der Gültigkeitszeiträume aller dieser Zertifikate liegen.

Werden Sperrauskünfte berücksichtigt, so muss der Zeitpunkt t_0 ebenfalls innerhalb deren Gültigkeitszeitraum liegen.

Fig. 8 zeigt, dass für alle vom Wurzelzertifikat MTACert direkt abhängigen Zertifikate, hier beispielsweise MACert1, eine Sperrliste (Certificate Revocation List, CRL) während des Prüfverfahrens eingeholt wurde. Diese Sperrliste kann nach PKIX zum Beispiel mit dem zu MTACert gehörenden MTAKey signiert worden sein. Weil üblicherweise der Schlüssel für Wurzelinstanzen sehr selten verwendet und ansonsten sicher außerhalb des operativen Betriebes verwahrt wird, hat eine Sperrliste, die von der Wurzelinstanz herausgegeben wurde,

im praktischen Betrieb oftmals eine relativ lange Gültigkeitsdauer 815 zum Beispiel von Tagen. Für alle anderen Zertifikate werden in der Regel einzelne Sperrauskünfte bezogen auf dieses Zertifikat jeweils von der ausstellenden Instanz auf Anfrage, zum Beispiel per OCSP, bereitgestellt, deren Datenvolumen relativ gering ist. Ihr Gültigkeitszeitraum 825 ist relativ kurz, zum Beispiel eine Stunde.

Ursprünglich wurde die Prüfung von Zertifikatsketten nicht für die langfristige Verifikation von Zertifikaten vorgesehen. Das Prüfverfahren ist für die Ad-hoc-
5 Verifikation der Identität von Kommunikationspartnern beim Verbindungsaufbau optimiert. Für Gerätezertifikate eignet es sich ohne weitere Modifikationen schon deshalb nicht, weil es besonders im industriellen Bereich schwierig ist, die maximale Lebensdauer von Geräten vorherzusehen und für
10 die üblicherweise langfristigen Zeiträume hinreichend starke und damit dauerhafte kryptographische Algorithmen zu verwenden, die von gängigen Implementierungen auch unterstützt werden. Nach PKIX-Standard ist zudem beispielsweise ein Wurzel- oder Sub-CA-Zertifikat mit einem
15 restlichen Gültigkeitszeitraum von 3 Jahren nicht geeignet, um davon abhängig noch Zertifikate mit einem Gültigkeitszeitraum von 5 Jahren auszustellen, weil der Gültigkeitszeitraum abhängiger Zertifikate innerhalb des Gültigkeitszeitraums des übergeordneten Zertifikates liegen
20 muss.

Die Erfindung sieht dementsprechend im Unterschied zum PKIX-Standard insbesondere vor, dass Zustandsauskünfte Positivnachweise erbringen und/oder Zertifikate nur zu dem
25 Zeitpunkt der Ausstellung damit zu prüfender Signaturen gültig gewesen sein müssen. Der zweite Punkt ermöglicht, dass der Gültigkeitszeitraum von Zertifikaten nicht innerhalb des Gültigkeitszeitraumes des Zertifikates des Ausstellers liegen muss, sondern länger sein kann.

30

Durch die Erfindung sollen im Idealfall Zertifikate automatisch als Fälschung erkannt werden, die unter

unautorisierter Verwendung der zugehörigen Signierschlüssel erzeugt wurden.

Der absichtliche oder versehentliche Missbrauch von
5 Manufacturer Attestation Keys (MAKeys), wie sie oben
beschrieben sind, stellt ein relativ hohes Risiko für den
Gerätehersteller dar. Denn die MAKeys sind üblicherweise in
großen Produktionshallen mit komplexen IT-Netzwerken in
Verwendung. Zwar können MAKeys mit Hilfe von sicheren
10 Signaturerstellungseinheiten wie sogenannte Crypto-Tokens
oder Smart-Cards sicher verwahrt werden, so dass ein
Kopieren des privaten Anteils mit einer vernachlässigbaren
Restwahrscheinlichkeit unmöglich ist. Dennoch besteht die
Gefahr, dass die Schlüssel unbefugt verwendet werden.
15 Insbesondere bei Auftragsfertigungen außerhalb der direkten
Kontrolle eines Rechteinhabers besteht die reale Gefahr der
Überproduktion und des Verkaufs der Ware auf eigene
Rechnung. Es besteht das Risiko des Schadens durch
entgangenes Geschäft. Wenn die Plagiate auch noch von
20 minderer Qualität sind, entsteht zusätzliches Risiko durch
die erhöhte Wahrscheinlichkeit von Produkthaftungsfällen
und das Risiko des Imageverlustes.

Durch die Erfindung wird eine kostengünstige Vorsorge
25 bereitgestellt für den Fall der Kompromittierung von
Signierschlüsseln, wie zum Beispiel MAKey1, MAKey2, MAKey3,
etc., zur Erstellung von Gerätezertifikaten.

Insbesondere können Plagiate ohne außerordentliche
30 Maßnahmen des legitimen Geräteherstellers oder
Rechteinhabers als solche erkannt werden, obwohl sie mit

einem Gerätezertifikat versehen sind, das missbräuchlich mit einem korrekten Signierschlüssel erstellt wurde.

5 Insbesondere im industriellen Bereich besteht ferner die Gefahr der missbräuchlichen Verwendung von Device Owner Attestation Keys (DOAKeys) wie sie oben beschrieben sind. Denn an einer Vielzahl von industriellen Standorten ist eine Vielzahl von Geräten im Einsatz, so dass mit relativ hoher Frequenz Ersatzgeräte in Betrieb genommen oder neue
10 hinzugefügt werden müssen. Entsprechend müssen für den praktikablen Einsatz Geräte vor Ort mit Gerätezertifikaten versorgt werden können und deshalb befinden sich manche DOAKeys im Feldeinsatz, wo die Überwachung ihrer Verwendung nicht immer mit größter Sorgfalt möglich ist.

15 Die Erfindung stellt für dieses Anwendungsgebiet gleichfalls eine kostengünstige Vorsorge für den Fall der Kompromittierung von Signierschlüsseln zur Erstellung von Gerätezertifikaten, wie zum Beispiel DOAKey1, DOAKey2,
20 DOAKey3, etc., bereit.

Insbesondere erkennt der Gerätebesitzer ohne außerordentliche Maßnahmen, dass sich ein Gerät in seinem Besitz befindet, dessen Gerätezertifikat ohne seine
25 Zustimmung erstellt wurde, also zum Beispiel durch missbräuchliche Verwendung des korrekten Signierschlüssels. Für Angreifer ist es interessant, manipulierte Geräte in den Bestand eines Besitzers einzuschleusen. Für sie ist es umso vorteilhafter, wenn solche Geräte nicht erkannt
30 werden.

Die Erfindung sieht insbesondere die folgenden Varianten vor:

1. Das Prüfverfahren nach PKIX-Standard wird um das Erfordernis einer Zustandsauskunft für Gerätezertifikate
5 erweitert, wobei die Zustandsauskunft einen Positivnachweis der Existenz und Gültigkeit des Gerätezertifikates enthält.
2. Ein spezielles Gültigkeitsmodell für Gerätezertifikate wird angewendet, wobei auf das Erfordernis eines
10 Positivnachweises in der Zustandsauskunft zum Gerätezertifikat verzichtet wird. Als Ersatz dient ein elektronischer Zeitstempel, welcher den Ausstellungszeitpunkt des Gerätezertifikates dokumentiert und von einem anderen Signierschlüssel unterschrieben wurde als das Gerätezertifikat.
- 15 3. Gerätezertifikate werden zusammen mit einem Existenznachweis und einem Zeitstempel erstellt und es wird ein spezielles Gültigkeitsmodell angewendet. Diese Variante stellt somit eine Kombination der ersten zwei Varianten dar.

20

Insbesondere für die zweite und dritte Variante sieht die Erfindung ferner mit besonderem Vorteil vor, die Prüfung der Gerätezertifikate ohne die Notwendigkeit zur Einholung von weiteren Zustandsinformationen zu Zertifikaten und
25 daher unabhängig von Kommunikationsnetzen zu ermöglichen.

Die nachfolgend beschriebene Variante der Erfindung basiert auf einer Kombination der Prüfung von Gerätezertifikaten nach PKIX-Standard mit dem zusätzlichen Erfordernis einer
30 Zustandsauskunft über die Existenz des Gerätezertifikates.

Ein für diese Variante einsetzbares System zum Erstellen von Gerätezertifikaten ist beispielhaft in Fig. 5a dargestellt, und ein entsprechendes System zur Gültigkeitsprüfung zum Einsatz beim Gerätebesitzer ist
5 beispielhaft in Fig. 5b dargestellt.

Ein Verfahren zum Erstellen von Gerätezertifikaten in Verbindung mit einem entsprechenden Verfahren zur Prüfung der Gültigkeit eines so erstellten Gerätezertifikates,
10 umfasst beispielhaft die folgenden Schritte:

1. Ein Gerätehersteller produziert Geräte 101, 102 und 103 und stellt dabei mit Hilfe eines MAKey, im dargestellten Ausführungsbeispiel MAKey1, für jedes Gerät
15 ein Gerätezertifikat aus. Die Ausstellung eines Gerätezertifikates erfolgt dabei wie oben beschrieben.
2. Nach der Produktion und dem Test werden für die produzierte Charge von Geräten alle Gerätezertifikate in der Gerätedatenbank 300 des Herstellers hinterlegt. Hierbei
20 erfolgt eine Prüfung möglichst von unabhängiger Stelle, dass die Anzahl der produzierten Geräte zu dem Produktionsauftrag passt, und nur wenn die Anzahl passt, werden die Gerätezertifikate in die Datenbank aufgenommen.
3. Optional erzeugt ein Automatismus einen Auszug 310 aus
25 der Gerätedatenbank 300, in dem im Wesentlichen nur die Gerätezertifikate enthalten sind. Dieser Auszug wird durch übliche Datensicherheitsmaßnahmen geschützt. Er dient als Grundlage für einen Zertifikatsauskunftsdiens 350, den der Hersteller öffentlich zugänglich betreibt und der vom
30 Geräteeigentümer zur Prüfung von Gerätezertifikaten benötigt wird.

4. Die Geräte 101, 102 und 103 der Charge werden zum Verkauf freigegeben, zum Beispiel indem sie in das Warenlager des Herstellers überführt werden.

5. Eine Person empfängt ein Gerät 101, zum Beispiel durch eine Bestellung beim Hersteller und dessen Lieferung. Die Person wird damit zum Gerätebesitzer.

6. Der Gerätebesitzer prüft die Zertifikatskette des Gerätes 101 und die Bindung des EK-Zertifikates an das Gerät 101 mit einem vom Hersteller dokumentierten Verfahren unter Verwendung des Zertifikates MTACert als Vertrauensanker. Dieser Schritt ist oben im Detail beschrieben. Der Gerätebesitzer verwendet hierfür zum Beispiel ein Software-Werkzeug, welches das MTACert kennt oder welches er ihm bekannt macht. Das Software-Werkzeug kann zum Beispiel der Gerätehersteller zur Verfügung stellen.

7. Der Gerätebesitzer holt nach einem vom Gerätehersteller dokumentierten Verfahren bei einem Auskunftsdienst 350 des Geräteherstellers einen Existenznachweis für das Gerätezertifikat ein, zum Beispiel mit Hilfe eines Software-Werkzeuges über das Protokoll OCSP. Der Auskunftsdienst 350 schlägt das Zertifikat in dem Auszug 310 aus der Gerätedatenbank 300 nach oder direkt in der Gerätedatenbank 300 und stellt die gewünschte Auskunft bereit.

Die Verwendung eines Auszuges 310 aus der Gerätedatenbank 300 ist somit optional. Solch ein Auszug 310 wird vorteilhaft verwendet, damit ein öffentlicher Dienst nicht direkt auf eine unternehmensinterne Datenbank 300 zugreifen muss und damit Zugriffe auf den Dienst nicht direkt die Datenbank 300 belasten.

Die Schritte 6 und 7 werden zu einem Zeitpunkt nach Wahl des Gerätebesitzers durchgeführt und beliebig wiederholt.

Die Wirkung des oben beschriebenen Verfahrens wird
5 offensichtlich, wenn eine angenommene missbräuchliche
Verwendung eines korrekten MAKey1 zum Zwecke der Erstellung
von gefälschten Gerätezertifikaten betrachtet wird. Die
gefälschten Gerätezertifikate würden bei Schritt 2 nicht in
die Datenbank 300 eingefügt werden, zum Beispiel weil bei
10 dem Vergleich mit dem Produktionsauftrag eine Diskrepanz
auffällt oder weil die missbräuchliche Verwendung des
MAKey1 ohne Zugriffsmöglichkeit auf die Datenbank 300
geschieht, zum Beispiel außerhalb der Produktionsstätte.
Bei Schritt 7 fällt der Existenznachweis zum gefälschten
15 Gerätezertifikat negativ aus und der Gerätebesitzer erkennt
das Plagiat. Die Wirksamkeit des Verfahrens wird somit
insbesondere durch die Schritte 2 und 7 erreicht.

Das Verfahren schützt auch dann, wenn der MAKey1 nicht
20 entwendet oder kopiert, sondern sporadisch und unentdeckt
missbräuchlich verwendet wird.

Im Folgenden ist eine Variante des obigen Verfahrens
beschrieben, das sich besonders eignet, wenn Geräte von
25 einem Auftragnehmer des Inhabers an den Schutzrechten
produziert werden.

Ein für diese Variante einsetzbares System zum Erstellen
von Gerätezertifikaten ist beispielhaft in Fig. 6a
30 dargestellt, und ein entsprechendes System zur
Gültigkeitsprüfung zum Einsatz beim Gerätebesitzer ist
beispielhaft in Fig. 6b dargestellt.

Ein entsprechendes Verfahren zum Erstellen von
Gerätezettifikaten in Verbindung mit einem entsprechenden
Verfahren zur Prüfung der Gültigkeit eines so erstellten
5 Gerätezettifikates, umfasst beispielhaft die folgenden
Schritte:

1. Ein Auftragnehmer fertigt im Auftrag des
Schutzrechteinhabers bzw. Herstellers eine Charge von
10 Geräten 101, 102 und 103. Am Produktionsarbeitsplatz 200
wird mit Hilfe eines vom Hersteller bereitgestellten MAKey1
und zugehörigem MACert1 für jedes Gerät 101, 102 und 103
ein Gerätezettifikat ausgestellt.
2. Der Auftragnehmer pflegt eine partielle Datenbank 300
15 mit den EK-Zettifikaten aller von ihm produzierten Geräte
101, 102 und 103.
3. Der Auftragnehmer erstellt für jede Charge von Geräten
einen Auszug 310 aus dieser Datenbank 300, in dem die
Gerätezettifikate enthalten sind.
- 20 4. Der Auftragnehmer stellt dem Hersteller diese Auszüge
zur Verfügung.
5. Der Hersteller kontrolliert die Auszüge, indem er sie
mit den von ihm vergebenen Produktionsaufträgen mit Hilfe
eines Kontrollsystems 320 vergleicht. Zum Beispiel
25 akzeptiert er Auszüge 310 nur, wenn die Menge der
gemeldeten Geräte zu den Aufträgen passt. Nur in dem Fall
fügt er die Gerätezettifikate und eventuell weitere
Information seiner Gerätedatenbank 330 hinzu.
6. Optional erstellt der Hersteller einen Auszug 340 aus
30 seiner Gerätedatenbank 330 zur Verwendung für den
Auskunftsdienst 350, den er zu seinen Gerätezettifikaten
betreibt.

7. Die Charge der neu produzierten Geräte wird nach der Kontrolle durch den Hersteller zum Vertrieb freigegeben, zum Beispiel indem sie in das Warenlager beim Auftragnehmer übernommen werden.

5 8. Eine Person empfängt ein Gerät 101, zum Beispiel durch Bestellung beim Hersteller und Auslieferung durch den Auftragnehmer. Die Person wird damit zum Gerätebesitzer.

9. Der Gerätebesitzer prüft die Echtheit des Gerätes 101 durch Prüfung der Zertifikatskette und Prüfung der Bindung
10 des EK-Zertifikates an das Gerät 101 wie oben beschrieben.

10. Der Gerätebesitzer holt einen Existenznachweis zum Gerätezertifikat beim Hersteller ein, wie oben beschrieben. Die Sicherheit des Verfahrens liegt hier analog zu der vorher beschriebenen Variante insbesondere in den Schritten

15 5 und 10. Die Kontrolle der Anzahl der Gerätezertifikate beim Hersteller als Auftraggeber vor deren Einfügung in seine Gerätedatenbank 330 ist für die Variante des Verfahrens wesentlich, denn damit wird die unautorisierte Überproduktion von Geräten verhindert. Hinzu kommt, dass
20 der Gerätebesitzer den Existenznachweis exakt bei demjenigen Auskunftsdienst 350 einholt, welchen der Hersteller unter seiner Kontrolle hat. Zum Beispiel ist das Verfahren zum Einholen des Existenznachweises in der Dokumentation zu den Geräten entsprechend offensichtlich
25 beschrieben oder das Software-Werkzeug zum Prüfen der Gerätezertifikate stammt vom Hersteller und verwendet nur den Auskunftsdienst 350 des Herstellers.

Die oben beschriebenen Verfahren zum Existenznachweis für
30 Echtheitszertifikate können analog auch für Besitzzertifikate verwendet werden, wobei dann die folgenden Modifikationen vorgesehen sind:

- Der Gerätebesitzer produziert die Geräte nicht, sondern personalisiert sie lediglich durch Kennzeichnung mit Besitzzertifikaten.
- Nicht der Gerätehersteller oder Auftragnehmer erstellt
5 die Gerätezertifikate, sondern der Gerätebesitzer mit Hilfe eines DOAKey wie oben beschrieben.
- Nicht der Gerätehersteller oder Auftragnehmer pflegt eine Gerätedatenbank mit den Gerätezertifikaten, sondern der Gerätebesitzer.
- 10 • Nicht der Gerätehersteller betreibt einen Zertifikatsauskunftsdiensdt für Existenznachweise zu den Gerätezertifikaten, sondern der Gerätebesitzer.
- Nicht der Gerätehersteller stellt das Wurzelzertifikat als Vertrauensanker, sondern der Gerätebesitzer durch sein
15 DOTACert.

Der Gerätebesitzer trägt also zur Stärke des Verfahrens mit der Strenge der Befolgung der Schritte innerhalb seiner Organisation bei. Für die Wirksamkeit des Verfahrens kann
20 ferner vorgesehen sein, die Kontrolle vor dem Einfügen von Gerätezertifikaten in die Gerätedatenbank von dem Schritt der Ausstellung von Gerätezertifikaten mittels DOAKey zu trennen. Insbesondere dient ein DOAKey nicht als Berechtigungskriterium, um Zertifikate in die
25 Gerätedatenbank hinzuzufügen.

In einer weiteren Variante der Erfindung ist eine Kombination eines speziellen Gültigkeitsmodells mit einem Nachweis, dass ein Zertifikat vor einem bestimmten
30 Zeitpunkt erzeugt wurde, vorgesehen. Dieser Nachweis wird als Zeitstempel bezeichnet, wobei ein mögliches Format für elektronische Zeitstempel beispielsweise in „RFC 3161

Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)", Internet Engineering Task Force (IETF), 2001, beschrieben wird. In diesem beispielhaften Format wird ein Hash-Wert eines existierenden Dokumentes zusammen
5 mit einem Datum und einer Zeitangabe von einer vertrauenswürdigen Stelle elektronisch signiert.

Der Unterschied dieser Erfindungsvariante zum oben beschriebenen Existenznachweis besteht in zwei Punkten:

10 1. Der Zeitstempel wird zum Zeitpunkt der Erzeugung des Gerätezertifikates oder kurz danach erzeugt, während der Existenznachweis zum Zeitpunkt der Prüfung des Gerätezertifikates erzeugt wird. Ein Existenznachweis ist nicht erforderlich. Eine Sperrauskunft ist hinreichend.

15 2. Die Prüfung der Gültigkeit des Zertifikates des Ausstellers (Sub-CA-Zertifikat) des Gerätezertifikates erfolgt nicht für den Zeitpunkt der Prüfung des Gerätezertifikates, sondern für den Zeitpunkt der Ausstellung des Gerätezertifikates.

20 Als Folge aus diesen Unterschieden können durch die Anwendung des Verfahrens nur solche Gerätezertifikate als gefälscht erkannt werden, die nach Sperrung des Sub-CA-Zertifikates unter Verwendung des korrekten Schlüssels
25 erstellt wurden. Eine Sperrung erfolgt zum Beispiel nach der Entdeckung der Kompromittierung eines solchen Schlüssels. Das Verfahren erlaubt also die Begrenzung des wirtschaftlichen Schadens aber nicht ganz seine Verhinderung. Dafür ist seine Anwendung gegebenenfalls
30 kostengünstiger als die Verwendung eines Existenznachweises.

Diese Variante der Erfindung wird im Folgenden näher beschrieben. Bei der folgenden Beschreibung des Verfahrens entsprechen die Bezeichnungen Produktionsstätte, Hersteller und Kunde Platzhaltern. Ein Hersteller ist der Inhaber an
5 Schutzrechten zu Geräten, welche in seinem Auftrag hergestellt werden. Der Hersteller beherrscht entweder die Produktionsstätte und produziert damit selbst oder die Produktionsstätte gehört einem Auftragnehmer, welcher im Auftrage des Herstellers Geräte produziert. Ein Kunde ist
10 eine Person, die in den Besitz eines Gerätes gelangt. Es ist dabei unerheblich, ob das Gerät direkt vom Hersteller erworben wurde.

Ein für diese Variante einsetzbares System zum Erstellen
15 von Gerätezertifikaten ist beispielhaft in Fig. 7a dargestellt, und ein entsprechendes System zur Gültigkeitsprüfung zum Einsatz beim Gerätebesitzer ist beispielhaft in Fig. 7b dargestellt.

20 Ein entsprechendes Verfahren zum Erstellen von Gerätezertifikaten in Verbindung mit einem entsprechenden Verfahren zur Prüfung der Gültigkeit eines so erstellten Gerätezertifikates, umfasst beispielhaft die folgenden Schritte:

25

1. Der Hersteller weist die Produktionsstätte an, eine bestimmte Anzahl Geräte 101, 102 und 103 zu produzieren. Optional hinterlegt er den Produktionsauftrag in seiner Auftragsdatenbank 370, zum Beispiel unter Verwendung eines
30 Enterprise-Resource-Planning-Systems (ERP-System).
2. Am Produktionsarbeitsplatz wird eine Charge von Geräten 101, 102 und 103 gefertigt.

3. Dabei wird je Gerät ein individuelles Gerätezertifikat erzeugt, wozu am Produktionsarbeitsplatz 200 ein MAKey, im dargestellten Beispiel MAKey1, zur Verfügung steht.
4. Für jedes erstellte Gerätezertifikat oder für alle Gerätezertifikate einer Charge zusammen werden Zeitstempel bei einem Zeitstempeldienst 360 angefordert. Der Zeitstempeldienst 360 kann hierzu vom Hersteller selbst betrieben werden oder aber von einer anderen vertrauenswürdigen Stelle.
5. Optional prüft der Zeitstempeldienst 360, ob ein hinreichender Produktionsauftrag in der Auftragsdatenbank 370 des Herstellers vorliegt.
6. Der Zeitstempeldienst 360 erstellt einen Zeitstempel. Jedem Gerät 101, 102 und 103 wird eine Kopie des zu seinem Gerätezertifikat zugeordneten Zeitstempels beigelegt. Zum Beispiel wird der Zeitstempel im Gerät in der Nähe des Gerätezertifikates in einem Speicher 121, 122 bzw. 123 gespeichert.
7. Das Gerät 101, 102 bzw. 103 wird zum Vertrieb freigegeben, zum Beispiel indem es in das Warenlager überführt wird.
8. Eine Person erwirbt ein Gerät 101 und wird damit zum Geräteinhaber.
9. Der Gerätebesitzer prüft die Zertifikatskette des Gerätes 101 und die Bindung des EK-Zertifikates an das Gerät 101 mit einem vom Hersteller dokumentierten Verfahren unter Verwendung des Zertifikates MTACert als Vertrauensanker. Dieser Schritt ist oben im Detail beschrieben. Die Prüfung der Zertifikatskette erfolgt durch ein spezielles Gültigkeitsmodell unter Verwendung von Informationen aus dem zum Gerätezertifikat gehörenden Zeitstempel, wie es weiter unten näher beschrieben wird.

Der Gerätebesitzer verwendet hierfür zum Beispiel ein Software-Werkzeug, welches das MTACert kennt oder welches er ihm bekannt macht. Das Software-Werkzeug kann zum Beispiel der Gerätehersteller zur Verfügung stellen.

5

Das bei dem oben beschriebenen Schritt 9 genannte spezielle Gültigkeitsmodell für die Prüfung einer Zertifikatskette ist in Fig. 9 dargestellt und wird nachfolgend beschrieben. In Fig. 9 sind Gültigkeitszeiträume 910, 920 und 930 für eine Zertifikatskette aus nur drei Zertifikaten dargestellt, es können aber prinzipiell eine beliebige Anzahl Zwischenzertifikate (Sub-CA-Zertifikate) vorgesehen sein.

15 Das spezielle Gültigkeitsmodell sieht folgende Schritte vor:

9.1. Zunächst wird der zum Gerätezertifikat gehörende Zeitstempel nach den Regeln seines Ausstellers auf Gültigkeit überprüft und seine Bindung an das Gerätezertifikat verifiziert.

20 9.2. Der Zeitpunkt t_0 der Prüfung des Gerätezertifikates muss innerhalb des Gültigkeitszeitraumes 930 des Gerätezertifikates liegen.

9.3. Der Zeitpunkt t_1 der Ausstellung des Zeitstempels wie er im Zeitstempel angegeben ist, muss innerhalb des Gültigkeitszeitraumes aller Zertifikate der Zertifikatskette und vor t_0 liegen.

25 9.4. Zu jedem Zwischenzertifikat der Zertifikatskette muss eine Sperrinformation vorliegen, die für den Zeitpunkt t_1 gültig ist, d.h. t_1 muss innerhalb des Gültigkeitszeitraums 915 der Sperrinformation liegen. Die Sperrinformation braucht keine Existenzinformation zu dem jeweiligen

30

Zertifikat auszuweisen, aber sie muss bestätigen, dass das zugehörige Zertifikat zum Zeitpunkt t_1 nicht gesperrt war.

Es ist also akzeptabel, wenn das Zertifikat zu einem Zeitpunkt nach t_1 gesperrt wurde. Der zuständige

5 Zertifizierungsdienst muss hierfür eine Sperrpolitik verfolgen, bei der Sperrungen nur mit einer Gültigkeit ab dem aktuellen Zeitpunkt erfolgen aber nie wieder aufgehoben werden können.

Das oben beschriebene Gültigkeitsmodell bedeutet effektiv,
10 dass ein Gerätezertifikat so lange als gültig verifiziert wird, bis sein Gültigkeitszeitraum 930 oder der Gültigkeitszeitraum des zugehörigen Zeitstempels abgelaufen ist, was immer zuerst eintritt. Diese beiden Gültigkeitszeiträume sollten vom Gerätehersteller
15 vorzugsweise auf die erwartete Nutzungsdauer des Gerätes und die erwartete Dauer der Widerstandsfähigkeit der bei den Zertifikaten und beim Zeitstempel verwendeten Algorithmen abgestimmt werden.

20 Für eine ausreichende Sicherheit des zuletzt oben beschriebenen Verfahrens ist die Erfüllung der folgenden Bedingungen vorgesehen:

a) Sobald eine unberechtigte Verwendung von Schlüsseln zur Erzeugung von Gerätezertifikaten entdeckt oder vermutet
25 wird, werden die zugehörigen Sub-CA-Zertifikate mit Wirksamkeit ab diesem Zeitpunkt unwiderruflich gesperrt. Dieses muss durch den Betreiber des zugehörigen Zertifizierungsdienstes und den berechtigten Nutzer der Schlüssel garantiert werden.

30 b) Der Zeitstempeldienst erstellt immer nur Zeitstempel für die aktuell gültige Zeit. Dieses wird durch jeden seriösen Zeitstempeldienst garantiert.

c) Der Zeitstempeldienst darf keinen Schlüssel zur Ausstellung von Zeitstempeln verwenden, der auch zum Ausstellen von Gerätezertifikaten verwendet wird.

5 d) Der Sperrauskunftsdiensd darf keinen Schlüssel zur Ausstellung von Auskünften verwenden, der auch zum Ausstellen von Gerätezertifikaten verwendet wird.

Unter der Annahme, dass kein Unberechtigter gültige Zeitstempel ausstellen kann, kann ein Unberechtigter
10 maximal bis zum Entdecken der unberechtigten Ausstellung von Gerätezertifikaten solche erfolgreich fälschen. Der wirtschaftliche Schaden lässt sich somit begrenzen, sobald er erkannt ist.

15 Die Verfahren zum Erstellen und Prüfen für Echtheitszertifikate wie zuletzt oben beschrieben, können analog für Besitzzertifikate verwendet werden, wobei die folgenden Modifikationen vorgesehen sind:

- Der Gerätebesitzer produziert die Geräte nicht,
20 sondern personalisiert sie lediglich durch Kennzeichnung mit Besitzzertifikaten.
- Nicht die Produktionsstätte erstellt die Gerätezertifikate, sondern der Gerätebesitzer mit Hilfe eines DOAKey wie in Abschnitt 3.2 oben beschrieben.
- 25 • Nicht die Produktionsstätte fordert die Zeitstempel an, sondern der Gerätebesitzer.
- Der Zeitstempeldienst wird nicht vom Gerätehersteller ausgewählt, sondern vom Gerätebesitzer.
- Nicht der Gerätehersteller, sondern der Gerätebesitzer
30 betreibt einen Sperrauskunftsdiensd für Zwischenzertifikate (Sub-CA-Zertifikate) der Zertifikatsketten der Gerätezertifikate.

- Nicht der Gerätehersteller stellt das Wurzelzertifikat als Vertrauensanker, sondern der Gerätebesitzer durch sein DOTACert.

5 Aus der Beschreibung des obigen Gültigkeitsmodells ist ersichtlich, dass alle einzuholenden Sperrinformationen nur für den Zeitpunkt t_1 der Erstellung des Zeitstempels gültig sein müssen. Das gilt auch für spätere Zeitpunkte, zu denen die Prüfung des Gerätezertifikates wiederholt wird. Es ist
10 also möglich, einmalig alle Zustandsinformationen einzuholen und sie später wiederzuverwenden. Ein Gerätehersteller kann diese Zustandsinformationen den von ihm ausgestellten Echtheitszertifikaten beifügen. Ein Gerätebesitzer kann das analog für von ihm ausgestellte
15 Besitzzertifikate tun. Diese Erweiterung ermöglicht eine spätere Prüfung von Gerätezertifikaten ohne Zugang zu einem Kommunikationsnetz, d.h. off-line. Diese Erweiterung wird unten noch detaillierter aber ganz analog für die nachfolgend beschriebene weitere Erfindungsvariante
20 beschrieben.

In der nachfolgend beschriebenen weiteren Erfindungsvariante ist vorgesehen, das Gerätezertifikat mit einem Zeitstempel zur Bestätigung des Zeitpunktes seiner
25 Ausstellung zu kombinieren, sowie desweiteren das Gerätezertifikat mittels eines Gültigkeitsmodells zu prüfen, welches Existenznachweise für die Zertifikate außer dem Wurzelzertifikat vorsieht.

30 Dies entspricht im Wesentlichen einer Kombination oben bereits beschriebener Erfindungsvarianten, wobei insbesondere vorteilhaft ermöglicht wird, dass durch

bestimmte Vorkehrungen bei der Erzeugung von Gerätezertifikaten ihre Prüfung später ohne weitere Einholung von Zusatzinformation erfolgen kann.

- 5 Jede benötigte Zusatzinformation kann mit dem Gerät ausgeliefert beziehungsweise in oder bei ihm aufbewahrt werden. Insbesondere kann damit die Prüfung unabhängig von Zugängen zu Kommunikationsnetzen wie dem Internet, also off-line, erfolgen.

10

Unabhängig davon, ob Gerätezertifikate als Echtheitszertifikate oder als Besitzzertifikate erstellt werden, sieht ein Verfahren zum Erstellen von Gerätezertifikaten und zum Prüfen von deren Gültigkeit unter Bezugnahme auf Fig. 10 vor, dass für jedes Gerätezertifikat Folgendes geschieht beziehungsweise gilt:

15

1. Nach der Erstellung eines Gerätezertifikates und vor seiner ersten Prüfung wird ein Zeitstempel zu dem Gerätezertifikat erzeugt. Gegebenenfalls wird der Zeitstempel zu einer Menge von Gerätezertifikaten erzeugt, zum Beispiel einer Charge von Geräten.

20

2. Bei jedem Prüfen der Gültigkeit von Gerätezertifikaten werden folgende Bedingungen geprüft:

25

2.1. Die Bindung des Gerätezertifikates an einen geheimen Schlüssel muss nachgewiesen werden.

2.2. Eine Zertifikatskette muss vom Gerätezertifikat zu einem Vertrauenswürdigen Wurzelzertifikat konstruiert werden können.

30

2.3. Der Zeitpunkt t_0 der Prüfung muss innerhalb des Gültigkeitszeitraumes 960 des Gerätezertifikates liegen.

2.4. Der Zeitstempel zum Gerätezertifikat muss nach den Regeln des Erstellers auf Gültigkeit geprüft werden. Dies

schließt insbesondere eine Prüfung der Bindung des Zeitstempels an das Gerätezertifikat ein.

2.5. Der Zeitpunkt t_1 der Erstellung des Zeitstempels, wie er in dem Zeitstempel angegeben ist, muss innerhalb des
5 Gültigkeitszeitraumes 960 des Gerätezertifikates und vor dem Zeitpunkt t_0 liegen.

2.6. Eine Zustandsinformation für das Gerätezertifikat muss existieren, für den Zeitpunkt t_1 gültig sein, d.h. t_1 muss innerhalb des Gültigkeitszeitraumes 955 liegen, und für
10 diesen Zeitpunkt bestätigen,

2.6.1. dass das Gerätezertifikat von berechtigter Stelle ausgestellt wurde, d.h. einen Existenznachweis liefern, zum Beispiel weil es in der Datenbank des Ausstellers verzeichnet ist, und

15 2.6.2. dass das Gerätezertifikat zum Zeitpunkt t_1 nicht gesperrt war.

2.7. Für jedes Zwischenzertifikat der Zertifikatskette (jedes Sub-CA-Zertifikat) muss gelten,

2.7.1. dass der Ausstellungszeitpunkt t_N des in der
20 Kette direkt von ihm abhängigen Zertifikates, zum Beispiel dessen Beginn des Gültigkeitszeitraumes, innerhalb des Gültigkeitszeitraumes 950 des Zwischenzertifikates liegt, wobei dies im dargestellten Beispiel der Ausstellungszeitpunkt t_2 des Gerätezertifikates ist,

25 2.7.2. dass zu dem Zwischenzertifikat eine für den Zeitpunkt t_N gültige Zustandsinformation existiert, welche die Existenz des Zwischenzertifikates bestätigt (Existenznachweis) und, dass es zum Zeitpunkt t_N gültig war, dass also im dargestellten Beispiel t_2 innerhalb des
30 Gültigkeitszeitraumes 945 der Zustandsinformation zu dem Zwischenzertifikat liegt.

2.8. Der Zeitpunkt t_3 der Ausstellung des vom Wurzelzertifikat direkt abhängigen Zwischenzertifikates muss innerhalb des Gültigkeitszeitraumes 940 des Wurzelzertifikates liegen.

5

Das mit Punkt 2 oben beschriebene Gültigkeitsmodell ist in Fig. 10 veranschaulicht. Die dort dargestellten Gültigkeitszeiträume basieren auf einer Zertifikatskette bestehend aus 3 Zertifikaten. Das beschriebene Verfahren ist jedoch ebenso für Zertifikatsketten mit mehreren Zwischenzertifikaten (Sub-CA-Zertifikaten) anwendbar.

10

Die Sicherheit des Verfahrens besteht darin, dass von unberechtigter Stelle ausgestellte Gerätezertifikate erkannt werden an dem Fehlen eines Zeitstempels, an dem Fehlen eines Existenznachweises und/oder an einem Zeitstempel mit Ausstellungszeitpunkt nach der Sperrung des Zertifikates des ausstellenden Schlüssels.

15

Dafür ist vorteilhaft vorgesehen, dass die folgenden Bedingungen erfüllt werden:

20

a) Sobald eine unberechtigte Verwendung von Schlüsseln zur Erzeugung von Gerätezertifikaten entdeckt oder vermutet wird, werden die zugehörigen Sub-CA-Zertifikate mit Wirksamkeit ab diesem Zeitpunkt unwiderruflich gesperrt. Dieses muss durch den Betreiber des zugehörigen Zertifizierungsdienstes und den berechtigten Nutzer der Schlüssel garantiert werden.

25

b) Der Zeitstempeldienst erstellt immer nur Zeitstempel für die aktuell gültige Zeit. Dieses wird durch jeden seriösen Zeitstempeldienst garantiert.

30

c) Der Zeitstempeldienst darf keinen Schlüssel zur Ausstellung von Zeitstempeln verwenden, der auch zum Ausstellen von Gerätezertifikaten verwendet wird.

5 d) Der Zustandsinformationsdienst, welcher für die Zertifikate der Kette Sperrauskünfte und Existenznachweise erstellt, darf dazu keinen Schlüssel verwenden, der auch zum Ausstellen von Gerätezertifikaten verwendet wird.

10 Aus der Beschreibung des obigen Gültigkeitsmodells ist ersichtlich, dass alle zum Gerätezertifikat zusätzlich benötigten Informationen zum Zeitpunkt t_1 der Erstellung des Zeitstempels eingeholt werden können. Dieses betrifft auch Auskünfte und Nachweise, die zur Prüfung des Zeitstempels selbst notwendig sind. Diese Informationen
15 können dem Gerätezertifikat beigelegt werden. Sie brauchen dann nicht mehr während nachfolgender Prüfungen erneut eingeholt zu werden. Stattdessen kann die Prüfung mit Hilfe dieser Information jederzeit erneut nachvollzogen werden.

20 Das Verfahren zur Zusammenstellung der Information wird nachfolgend beispielhaft unter Bezugnahme auf die Figuren 11a und 11b beschrieben, um zu verdeutlichen, welche Information von woher stammen kann. Bei der folgenden Beschreibung des Verfahrens entsprechen die Bezeichnungen
25 Produktionsstätte, Hersteller und Kunde Platzhaltern. Ein Hersteller ist der Inhaber an Schutzrechten zu Geräten, welche in seinem Auftrag hergestellt werden. Der Hersteller beherrscht entweder die Produktionsstätte und produziert damit selbst oder die Produktionsstätte gehört einem
30 Auftragnehmer, welcher im Auftrage des Herstellers Geräte produziert. Ein Kunde ist eine Person, die in den Besitz

eines Gerätes gelangt. Es ist dabei unerheblich, ob das Gerät direkt vom Hersteller erworben wurde.

Ein Verfahren zum Erstellen von Gerätezertifikaten in
5 Verbindung mit einem entsprechenden Verfahren zur Prüfung der Gültigkeit eines so erstellten Gerätezertifikates umfasst in dieser Ausführungsvariante der Erfindung beispielhaft die folgenden Schritte:

- 10 1. Der Hersteller weist die Produktionsstätte an, eine bestimmte Anzahl Geräte 101, 102 und 103 zu produzieren. Optional hinterlegt er den Produktionsauftrag in einer, in Fig. 11a nicht dargestellten Auftragsdatenbank, zum Beispiel seinem Enterprise-Resource-Planning-System (ERP-
15 System).
2. Am Produktionsarbeitsplatz wird eine Charge von Geräten gefertigt.
3. Dabei wird je Gerät 101, 102 bzw. 103 ein individuelles Gerätezertifikat erzeugt, wozu am
20 Produktionsarbeitsplatz 200 ein MAKey1 zur Verfügung steht. Die Produktionsstätte sendet die Gerätezertifikate einer Charge an den Hersteller, beispielsweise unter Verwendung einer partiellen Datenbank 300 des Auftragnehmers und eines daraus erstellten Datenbankauszugs 310.
- 25 4. Beim Hersteller wird die Liste geprüft, zum Beispiel durch einen Vergleich mit der Auftragsdatenbank. Im Falle der positiven Prüfung werden die Gerätezertifikate in der Datenbank 330 des Herstellers hinterlegt.
5. Für jedes erstellte Gerätezertifikat oder für alle
30 Gerätezertifikate einer Charge zusammen werden Zeitstempel bei einem Zeitstempeldienst 370 angefordert. Der Zeitstempeldienst kann hierzu vom Hersteller selbst

betrieben werden oder aber von einer anderen vertrauenswürdigen Stelle. Zusätzlich wird zu jedem Gerätezertifikat oder für alle Zertifikate der Charge eine Zustandsauskunft mit Existenznachweis und Sperrinformation eingeholt. Diese stammt vom Hersteller. Der Zustandsauskunftsdienst 370 überprüft vor Auskunftserteilung die Existenz der Geräte anhand der Gerätedatenbank 330 oder eines Auszugs davon. Der Zeitstempel und die Zustandsauskunft werden den Geräten 101, 102 bzw. 103 beigelegt oder sogar in ihnen gespeichert, beispielsweise in einem Speicher 121, 122 bzw. 123.

6. Das Gerät wird zum Vertrieb freigegeben, zum Beispiel indem es in das Warenlager überführt wird.

7. Eine Person erwirbt ein Gerät 101 und wird damit zum Geräteinhaber.

8. Der Gerätebesitzer prüft die Zertifikatskette des Gerätes und die Bindung des EK-Zertifikates an das Gerät 101 mit einem vom Hersteller dokumentierten Verfahren unter Verwendung des Zertifikates MTACert als Vertrauensanker. Die Prüfung der Zertifikatskette erfolgt durch ein spezielles Gültigkeitsmodell wie oben beschrieben. Dabei werden die bereits vorhandenen Zustandsauskünfte und Zeitstempel verwendet. Der Gerätebesitzer verwendet hierfür zum Beispiel ein Software-Werkzeug, welches das MTACert kennt oder welches er ihm bekannt macht. Das Software-Werkzeug kann zum Beispiel der Gerätehersteller zur Verfügung stellen. Wie in Fig. 11b dargestellt, ist für die Prüfung somit vom Prüfcomputer 700 lediglich ein Zugriff auf das Gerät 101, nicht aber auf andere Informationsquellen erforderlich.

Das Zusammenstellen von Nachweisen für Besitzzertifikate erfolgt analog, wobei die folgenden Modifikationen vorgesehen sind:

- Der Gerätebesitzer produziert die Geräte nicht,
5 sondern personalisiert sie lediglich durch Kennzeichnung mit Besitzzertifikaten.
- Nicht die Produktionsstätte erstellt die Gerätezertifikate, sondern der Gerätebesitzer mit Hilfe eines DOAKey wie oben beschrieben.
- 10 • Nicht die Produktionsstätte fordert die Zeitstempel und Zustandsauskünfte an, sondern der Gerätebesitzer.
- Der Zeitstempeldienst wird nicht vom Gerätehersteller ausgewählt, sondern vom Gerätebesitzer.
- Nicht der Gerätehersteller, sondern der Gerätebesitzer
15 betreibt einen Sperrauskunftsdienst für Zwischenzertifikate (Sub-CA-Zertifikate) der Zertifikatsketten der Gerätezertifikate.
- Nicht der Gerätehersteller stellt das Wurzelzertifikat als Vertrauensanker, sondern der Gerätebesitzer durch sein
20 DOTACert.

Patentansprüche

1. Verfahren zum Erstellen von Gerätezertifikaten (630) für elektronische Geräte (101-103), umfassend die Schritte:

- 5 - Bereitstellen eines elektronischen Gerätes (101-103) mit einem darin gespeicherten, von außerhalb des Gerätes nicht auslesbaren Geheimnis,
- Erzeugen eines Gerätezertifikates (630), dessen Zertifikatsinformation (530) kryptographisch an das
- 10 Geheimnis gebunden ist, wobei das Gerätezertifikat (630) eine mit einem Signierschlüssel (525) erzeugte digitale Signatur (430) umfasst und mittels einer Zertifikatskette (610, 620, 630) authentisierbar ist, wobei die Zertifikatskette eine mit dem Gerätezertifikat (630)
- 15 beginnende Folge von wenigstens zwei Zertifikaten ist, wobei jedes Zertifikat (610, 620, 630) der Zertifikatskette eine Information umfasst, welche den Gültigkeitszeitraum des jeweiligen Zertifikates definiert, und wobei jedes Zertifikat (610, 620) der Zertifikatskette mit Ausnahme des
- 20 Gerätezertifikates (630) eine Zertifikatsinformation (510, 520) umfasst, mit welcher das jeweils in der Folge vorhergehende Zertifikat authentisierbar ist, und
- Erstellen einer Bestätigungsinformation, welche bestätigt, dass das Gerätezertifikat (630) von einer
- 25 autorisierten Instanz erzeugt wurde
- und/oder
- Erzeugen eines digital signierten Zeitstempels, welcher das Gerätezertifikat mit dem Zeitpunkt verknüpft, zu dem der Zeitstempel erzeugt wird.

30

2. Verfahren nach Anspruch 1, ferner umfassend den Schritt:

- Bereitstellen, unter Ansprechen auf die Bestätigungsinformation, einer digital signierten Zustandsinformation für das Gerätezertifikat (630), welche einen Nachweis umfasst, dass das Gerätezertifikat (630) von einer autorisierten Instanz erzeugt wurde.

3. Verfahren nach Anspruch 2, ferner umfassend den Schritt:

- Bereitstellen einer digital signierten Zustandsinformation für wenigstens ein weiteres Zertifikat der Zertifikatskette, welches den Nachweis umfasst, dass das weitere Zertifikat von einer autorisierten Instanz erzeugt wurde.

4. Verfahren nach einem der vorstehenden Ansprüche, wobei das erzeugte Gerätezertifikate (630) und/oder wenigstens ein weiteres Zertifikat der Zertifikatskette und/oder der digital signierte Zeitstempel und/oder wenigstens eine digital signierte Zustandsinformation in einer dem Gerät zuordenbaren Weise abrufbar bereitgestellt wird, insbesondere durch Speichern in einem auslesbaren Speicher (121-123) oder Speichermedium, welches dem elektronischen Gerät (101-103) zugeordnet oder im elektronischen Gerät (101-103) angeordnet ist, oder durch Bereitstellen mittels eines Verzeichnisdienstes.

5. Verfahren nach einem der vorstehenden Ansprüche, wobei

- der digital signierte Zeitstempel von einem Server (360, 370), welcher einen Zeitstempeldienst bereitstellt, in Antwort auf eine Anfrage zur Erstellung eines Zeitstempels erzeugt wird,
- die erzeugten Zeitstempel gezählt werden, und

- der Server (360, 370) den Zeitstempel nur erzeugt, solange eine vorgegebene Obergrenze für die Anzahl der erzeugten Zeitstempel nicht überschritten wird.

5 6. Verfahren nach einem der vorstehenden Ansprüche, wobei für die Erzeugung der digitalen Signatur (430) des Gerätezertifikates (630) und der digitalen Signatur des Zeitstempels unterschiedliche Signierschlüssel verwendet werden.

10

7. Verfahren nach einem der vorstehenden Ansprüche, wobei für die Erzeugung der digitalen Signatur des Gerätezertifikates und der digitalen Signatur der Zustandsinformationen unterschiedliche Signierschlüssel
15 verwendet werden.

8. Verfahren nach einem der vorstehenden Ansprüche, ferner umfassend die Schritte:
- Erkennen einer unberechtigten Verwendung eines zum
20 Signieren eines ersten Zertifikates (630) der Zertifikatskette verwendeten Signierschlüssels (525), und
- Erzeugen einer digital signierten Zustandsinformation für das in der Zertifikatskette auf das erste Zertifikat (630) folgende Zertifikat (620), wobei die Zustandsinformation
25 eine Sperrinformation umfasst, welche das in der Zertifikatskette auf das erste Zertifikat (630) folgende Zertifikat (620) für Prüfzeitpunkte ab dem Zeitpunkt, zu dem die unberechtigte Verwendung erkannt wurde, als ungültig identifiziert.

30

9. Verfahren nach einem der vorstehenden Ansprüche, wobei das Geheimnis der private Teil eines asymmetrischen Schlüsselpaares ist.

5 10. Verfahren nach einem der vorstehenden Ansprüche, wobei das Geheimnis in einem Chip (111-113) des Gerätes (101-103) gespeichert ist.

11. Verfahren zur Prüfung der Gültigkeit eines
10 Gerätezertifikates (630), insbesondere nach einem Verfahren gemäß einem der Ansprüche 1 bis 10 erstellten Gerätezertifikates (630), umfassend die Schritte:
- Bereitstellen eines Gerätezertifikates (630),
- Bereitstellen eines vertrauenswürdigen Zertifikates
15 (610), wobei das Gerätezertifikat (630) mit dem vertrauenswürdigen Zertifikat (610) über eine Zertifikatskette (630, 620, 610) verkettbar ist, wobei die Zertifikatskette eine mit dem Gerätezertifikat (630) beginnende und mit dem vertrauenswürdigen Zertifikat (610)
20 endende Folge von wenigstens zwei Zertifikaten ist, wobei jedes Zertifikat der Zertifikatskette eine Information umfasst, welche den Gültigkeitszeitraum des jeweiligen Zertifikates definiert, und wobei jedes Zertifikat (610, 620) der Zertifikatskette mit Ausnahme des
25 Gerätezertifikates (630) eine Zertifikatsinformation (520, 510) umfasst, mit welcher das jeweils in der Folge vorhergehende Zertifikat (620, 630) authentisierbar ist,
- Festlegen eines zugeordneten Prüfzeitpunktes für jedes Zertifikat (630, 620, 610) der Zertifikatskette,
30 - Bereitstellen einer dem Gerätezertifikat (630) zugeordneten, digital signierten Zustandsinformation, wobei die Zustandsinformation das Gerätezertifikat als gültig

oder ungültig identifiziert und eine Information umfasst,
welche den Gültigkeitszeitraum der Zustandsinformation
definiert,

- Festlegen eines zugeordneten Prüfzeitpunktes für die dem
5 Gerätezertifikat (630) zugeordnete Zustandsinformation,

- Prüfen,

- ob das Gerätezertifikat (630) mittels der
Zertifikatskette (630, 620, 610) erfolgreich
authentisierbar ist,

10 - ob für jedes Zertifikat (630, 620, 610) der
Zertifikatskette der zugeordnete Prüfzeitpunkt
innerhalb des Gültigkeitszeitraumes des jeweiligen
Zertifikates liegt,

- mittels eines in einem von außerhalb des Gerätes
15 (101-103) nicht auslesbaren Speicher des Gerätes (101-
103) hinterlegten Geheimnisses, ob eine Bindung des
Gerätezertifikates (630) an das Gerät besteht (101-
103),

- ob für die dem Gerätezertifikat (630) zugeordnete
20 Zustandsinformation der zugeordnete Prüfzeitpunkt
innerhalb des Gültigkeitszeitraumes der
Zustandsinformation liegt,

- ob die dem Gerätezertifikat (630) zugeordnete
Zustandsinformation das Gerätezertifikat als gültig
25 identifiziert, wobei die Kennzeichnung des
Gerätezertifikates als gültig den Nachweis umfasst,
dass das Gerätezertifikat (630) von einer autorisierten
Instanz erzeugt wurde,

wobei bei erfolgreicher Prüfung das Gerätezertifikat (630)
30 als gültig, andernfalls als ungültig erkannt wird.

12. Verfahren nach Anspruch 11, ferner umfassend die Schritte:

- Bereitstellen einer zugeordneten, digital signierten Zustandsinformation für wenigstens ein weiteres Zertifikat (620, 610) der Zertifikatskette, wobei die Zustandsinformation das weitere Zertifikat (620, 610) als gültig oder ungültig identifiziert und eine Information umfasst, welche den Gültigkeitszeitraum der Zustandsinformation definiert,
- Festlegen eines zugeordneten Prüfzeitpunktes für jede Zustandsinformation,
- Erkennen des Gerätezertifikates (630) als gültig, nur wenn
 - für jede Zustandsinformation der zugeordnete Prüfzeitpunkt innerhalb des Gültigkeitszeitraumes der jeweiligen Zustandsinformation liegt, und
 - jede Zustandsinformation das jeweils zugeordnete weitere Zertifikat als gültig identifiziert, wobei die Kennzeichnung des weiteren Zertifikates (620, 610) als gültig den Nachweis umfasst, dass das weitere Zertifikat (620, 610) von einer autorisierten Instanz erzeugt wurde.

13. Verfahren zur Prüfung der Gültigkeit eines Gerätezertifikates (630), insbesondere nach einem Verfahren gemäß einem der Ansprüche 1 bis 10 erstellten Gerätezertifikates (630), umfassend die Schritte:

- Bereitstellen eines Gerätezertifikates (630),
- Bereitstellen eines vertrauenswürdigen Zertifikates (610), wobei das Gerätezertifikat (630) mit dem vertrauenswürdigen Zertifikat (610) über eine Zertifikatskette (630, 620, 610) verkettbar ist, wobei die

Zertifikatskette eine mit dem Gerätezertifikat (630) beginnende und mit dem vertrauenswürdigen Zertifikat (610) endende Folge von wenigstens zwei Zertifikaten ist, wobei jedes Zertifikat der Zertifikatskette eine Information

5 umfasst, welche den Gültigkeitszeitraum des jeweiligen Zertifikates definiert, und wobei jedes Zertifikat (610, 620) der Zertifikatskette mit Ausnahme des Gerätezertifikates (630) eine Zertifikatsinformation (520, 510) umfasst, mit welcher das jeweils in der Folge

10 vorhergehende Zertifikat (620, 630) authentisierbar ist,

- Bereitstellen eines dem Gerätezertifikat zugeordneten digital signierten Zeitstempels, welcher das Gerätezertifikat (630) mit einem Zeitpunkt verknüpft,
- Festlegen eines zugeordneten Prüfzeitpunktes für jedes

15 Zertifikat (630, 620, 610) der Zertifikatskette, wobei als zugeordneter Prüfzeitpunkt für wenigstens eines der Zertifikate (630, 620, 610) der Zertifikatskette der über den Zeitstempel mit dem Gerätezertifikat (630) verknüpfte Zeitpunkt festgelegt wird,

20 - Prüfen,

- ob das Gerätezertifikat (630) mittels der Zertifikatskette (630, 620, 610) erfolgreich authentisierbar ist,
- ob der Zeitstempel erfolgreich authentisierbar ist,

25 - ob für jedes Zertifikat (630, 620, 610) der Zertifikatskette der zugeordnete Prüfzeitpunkt innerhalb des Gültigkeitszeitraumes des jeweiligen Zertifikates liegt,- mittels eines in einem von außerhalb des Gerätes

30 (101-103) nicht auslesbaren Speicher des Gerätes (101-103) hinterlegten Geheimnisses, ob eine Bindung des

Gerätezertifikates (630) an das Gerät besteht (101-103),

wobei bei erfolgreicher Prüfung das Gerätezertifikat (630) als gültig, andernfalls als ungültig erkannt wird.

5

14. Verfahren nach Anspruch 13, ferner umfassend die Schritte:

- Bereitstellen einer zugeordneten, digital signierten Zustandsinformation für wenigstens ein Zertifikat (630, 10 620, 610) der Zertifikatskette, wobei die Zustandsinformation das Zertifikat (630, 620, 610) als gültig oder ungültig identifiziert und eine Information umfasst, welche den Gültigkeitszeitraum der Zustandsinformation definiert,
- 15 - Festlegen eines zugeordneten Prüfzeitpunktes für jede Zustandsinformation,
- Erkennen des Gerätezertifikates (630) als gültig, nur wenn
 - für jede Zustandsinformation der zugeordnete 20 Prüfzeitpunkt innerhalb des Gültigkeitszeitraumes der jeweiligen Zustandsinformation liegt, und
 - jede Zustandsinformation das jeweils zugeordnete Zertifikat als gültig identifiziert, wobei die Kennzeichnung des Zertifikates (630, 620, 610) als 25 gültig den Nachweis umfasst, dass das Zertifikat (630, 620, 610) von einer autorisierten Instanz erzeugt wurde.

15. Verfahren nach einem der Ansprüche 11 bis 14, wobei 30 als zugeordneter Prüfzeitpunkt für wenigstens eines der Zertifikate (630, 620, 610) der Zertifikatskette und/oder wenigstens eine der Zustandinformationen der Zeitpunkt

festgelegt wird, zu dem die Prüfung der Gültigkeit des Gerätezertifikates (630) durchgeführt wird.

16. Verfahren nach einem der Ansprüche 11 bis 15, wobei
5 als zugeordneter Prüfzeitpunkt für wenigstens eine der Zustandinformationen der über den authentisierten Zeitstempel mit dem Gerätezertifikat verknüpfte Zeitpunkt festgelegt wird.

10 17. Verfahren nach einem der Ansprüche 11 bis 16, wobei als zugeordneter Prüfzeitpunkt für das Gerätezertifikat (630) der Zeitpunkt festgelegt wird, zu dem die Prüfung der Gültigkeit des Gerätezertifikates (630) durchgeführt wird, und wobei für alle weiteren Zertifikate (620, 610) der
15 Zertifikatskette der über einen Zeitstempel mit dem Gerätezertifikat (630) verknüpfte Zeitpunkt festgelegt wird.

18. Verfahren nach einem der Ansprüche 11 bis 17, wobei
20 als zugeordneter Prüfzeitpunkt für wenigstens eines der Zertifikate (630, 620, 610) der Zertifikatskette und/oder für die diesem Zertifikat zugeordnete Zustandsinformation der Zeitpunkt festgelegt wird, zu dem das in der Zertifikatskette vorhergehende Zertifikat erstellt wurde
25 oder zu dem der Gültigkeitszeitraum des in der Zertifikatskette vorhergehenden Zertifikates beginnt.

19. Verfahren nach einem der Ansprüche 11 bis 18, wobei
30 das Gerätezertifikat (630) die Funktion eines Echtheitszertifikates oder Besitzzertifikates aufweist und/oder das Gerätezertifikat (630) als Attributzertifikat ausgebildet ist.

20. Verfahren nach einem der Ansprüche 11 bis 19, wobei
die Zertifikatskette wenigstens ein Zwischenzertifikat
(620) umfasst, welches in der durch die Zertifikatskette
5 definierten Reihenfolge zwischen dem Gerätezertifikat (630)
und dem vertrauenswürdigen Zertifikat (610) angeordnet ist.

21. Verfahren nach einem der Ansprüche 11 bis 20, wobei
das vertrauenswürdige Zertifikat (610) ein selbstsigniertes
10 Wurzelzertifikat ist.

22. System zum Erstellen von Gerätezertifikaten (630) für
elektronische Geräte (101-103), ausgebildet zum Ausführen
eines Verfahrens gemäß einem der Ansprüche 1 bis 10,
15 umfassend

- einen Produktionscomputer (200) mit einem darin
gespeicherten Signierschlüssel zum Erzeugen von
Gerätezertifikaten (630) für elektronische Geräte (101-
103), dazu ausgebildet, auf einen Speicher (121-123) des
20 jeweiligen elektronischen Gerätes (101-103) zuzugreifen,
und
- eine mit dem Produktionscomputer (200) verbindbare
Datenbank (300, 310), in welcher der Produktionscomputer
(200) erzeugte Gerätezertifikate (630) oder daraus
25 abgeleitete Werte speichert, wobei die Datenbank (300, 310)
dazu ausgebildet ist, auf Anfrage eine Information
bereitzustellen, ob ein angefragtes Gerätezertifikat (630)
oder ein aus einem angefragten Gerätezertifikat (630)
abgeleiteter Wert in der Datenbank (300, 310) gespeichert
30 ist, und/oder
- ein mit dem Produktionscomputer (200) verbindbarer Server
(360, 370), welcher einen Zeitstempeldienst bereitstellt,

und welcher auf Anfrage des Produktionscomputers (200) für ein vom Produktionscomputer vorgegebenes Gerätezertifikat (630) einen digital signierten Zeitstempel erzeugt und dem Produktionscomputer (200) übermittelt, wobei der
5 Zeitstempel das vorgegebene Gerätezertifikat (630) mit dem Zeitpunkt verknüpft, zu dem der Zeitstempel erzeugt wird.

23. System zur Prüfung der Gültigkeit eines Gerätezertifikates (630), ausgebildet zum Durchführen eines
10 Verfahrens gemäß einem der Ansprüche 11 bis 21, umfassend
- ein Prüfgerät (700) zum Prüfen der Gültigkeit eines in einem Speicher eines elektronischen Gerätes hinterlegten Gerätezertifikates (630) mittels einer Zertifikatskette (630, 620, 610), und
15 - einen Zertifikatsauskunfts-Server (350, 370), auf welchen das Prüfgerät (700) zugreifen kann, um Zustandsinformationen für wenigstens ein Zertifikat (630, 620, 610) der Zertifikatskette abzufragen.

20 24. Elektronisches Gerät (101-103) mit einem von außerhalb des Gerätes nicht auslesbaren Speicher mit einem darin gespeicherten Geheimnis und mit einem auslesbaren Speicher (121-123), wobei in dem auslesbaren Speicher alle für die Durchführung eines Verfahrens gemäß einem der Ansprüche 11
25 bis 21 erforderlichen Informationen, insbesondere Zertifikate (630, 620) der Zertifikatskette, Zustandsinformationen und/oder Zeitstempel, gespeichert sind.

30 25. Speichermedium, welches einem elektronischen Gerät (101-103) zugeordnet ist, wobei das elektronische Gerät (101-103) einen von außerhalb des Gerätes nicht auslesbaren

Speicher mit einem darin gespeicherten Geheimnis umfasst,
und wobei in dem Speichermedium alle für die Durchführung
eines Verfahrens gemäß einem der Ansprüche 11 bis 21
erforderlichen Informationen, insbesondere Zertifikate
5 (630, 620) der Zertifikatskette, Zustandsinformationen
und/oder Zeitstempel, gespeichert sind.

Fig. 1

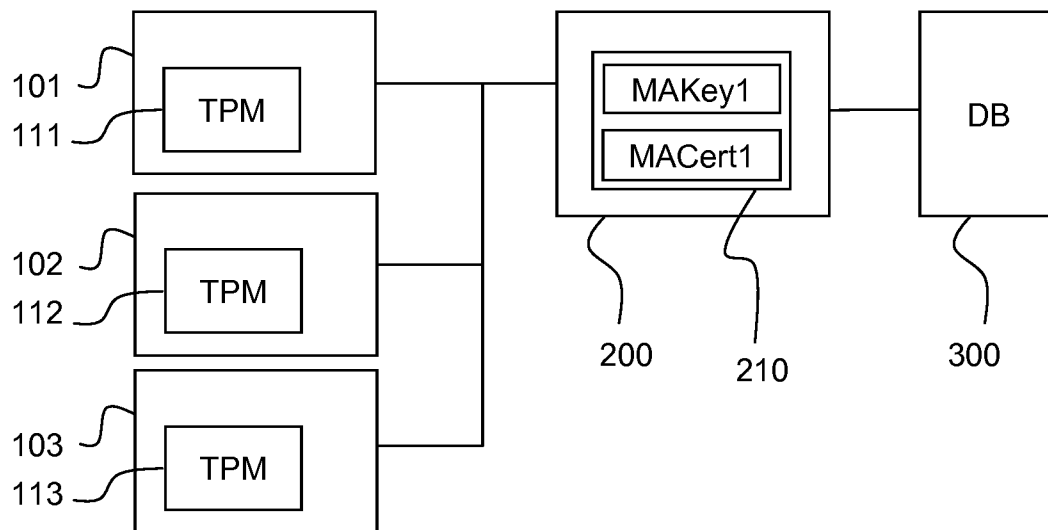


Fig. 2

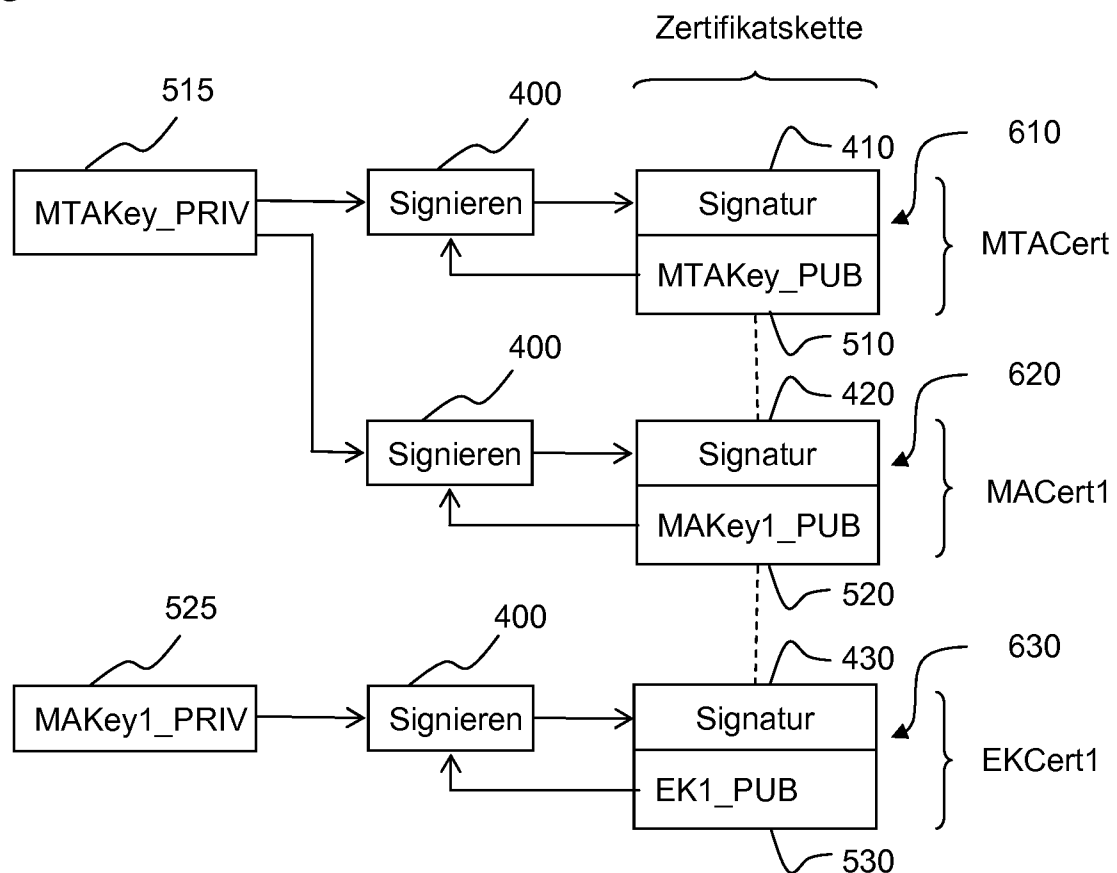


Fig. 3

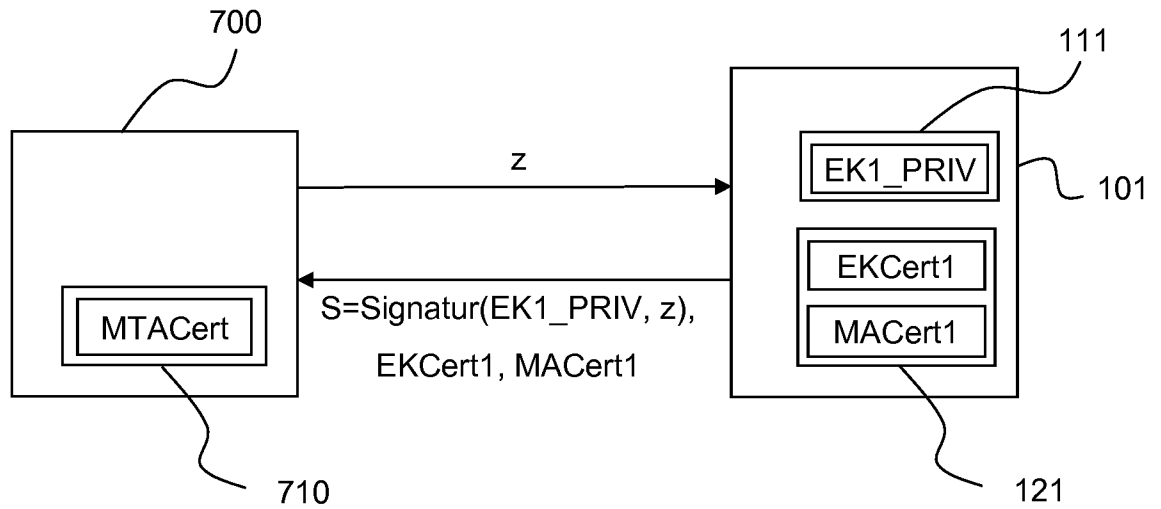


Fig. 4

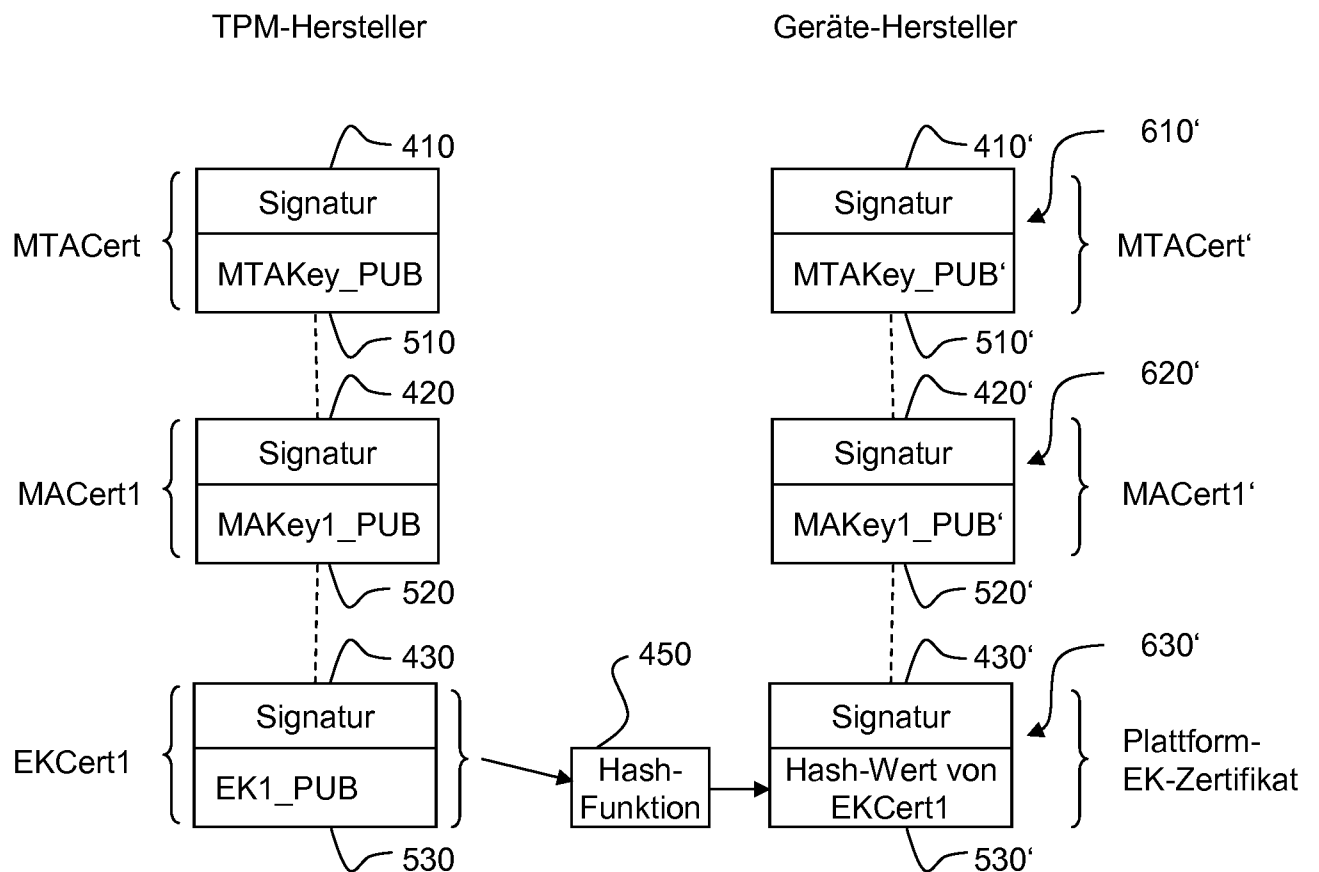


Fig. 5a

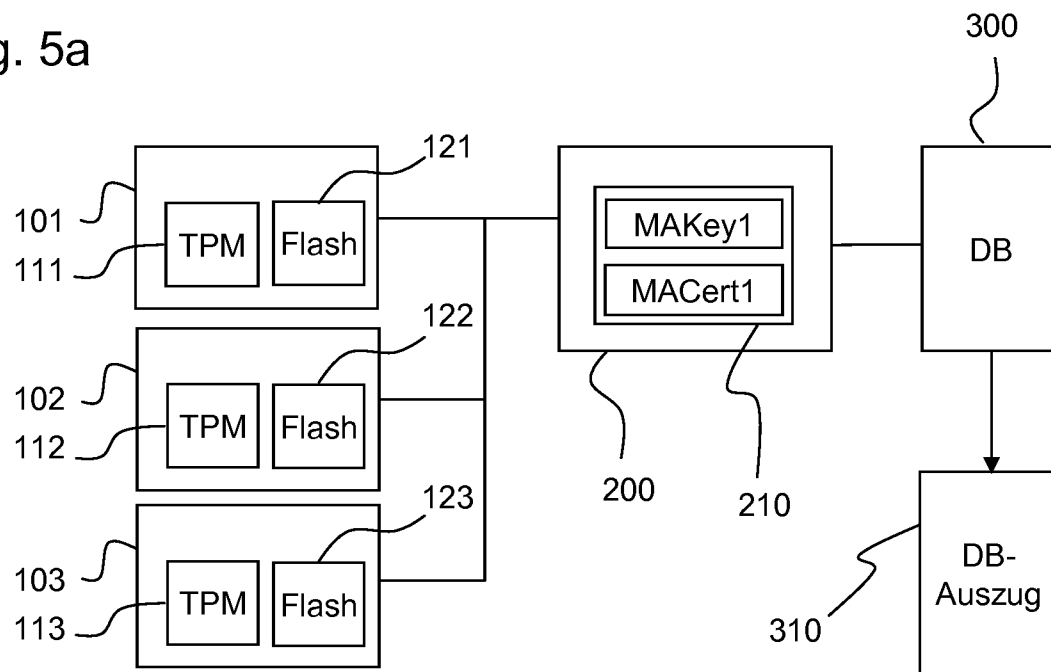


Fig. 5b

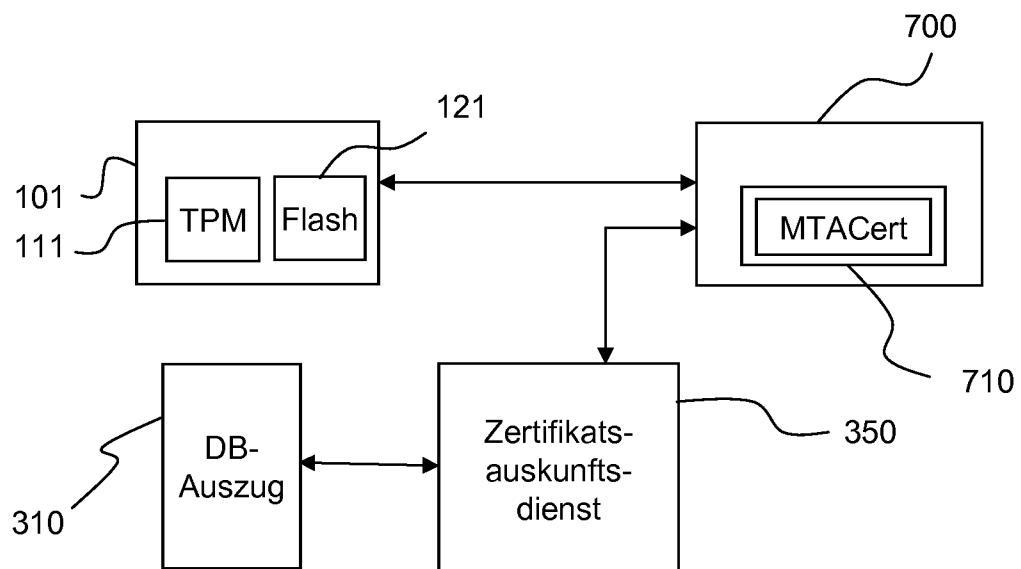


Fig. 6a

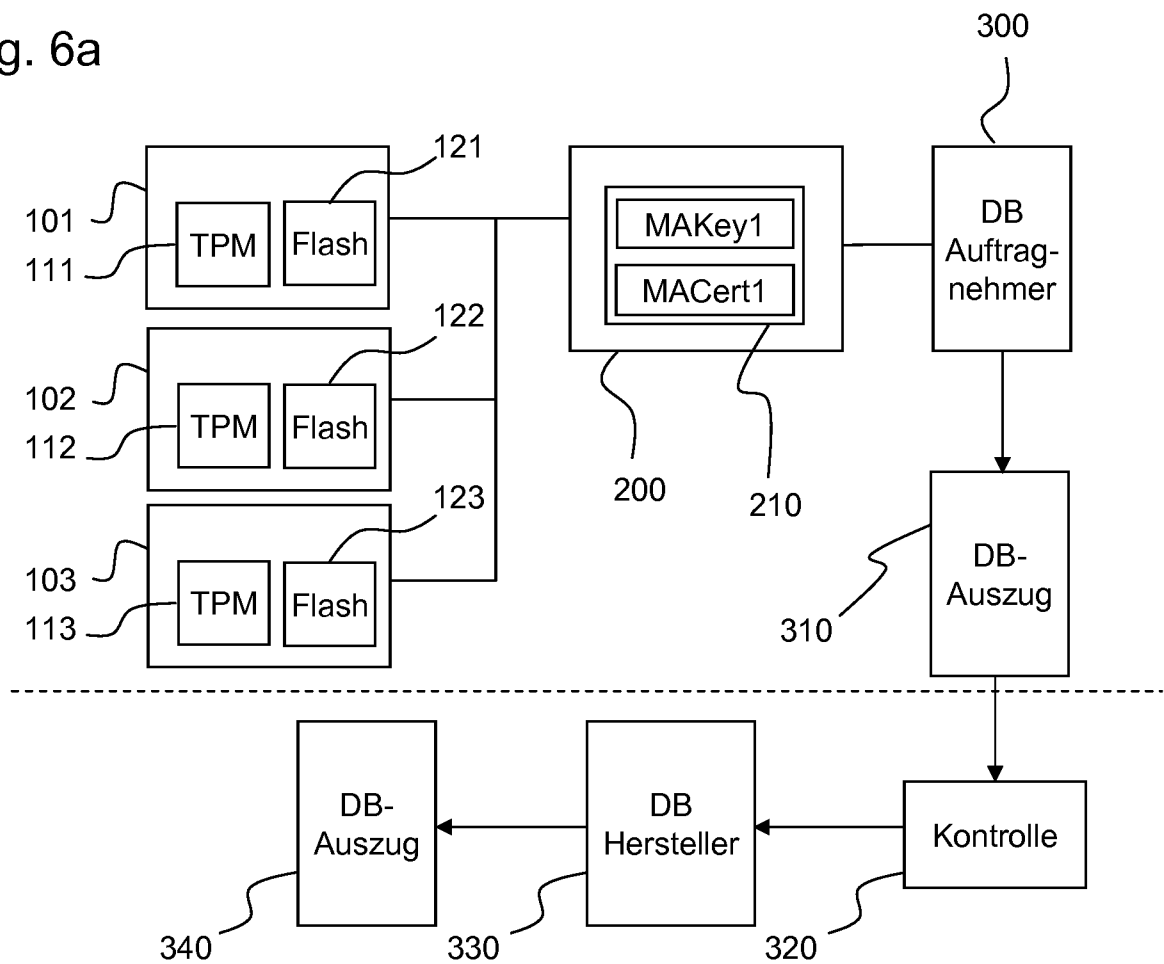


Fig. 6b

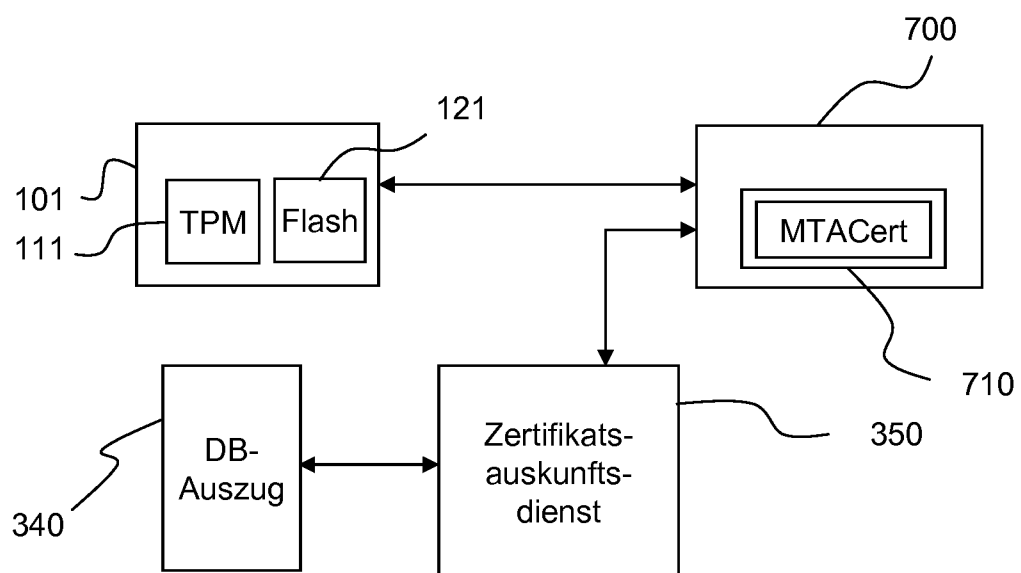


Fig. 7a

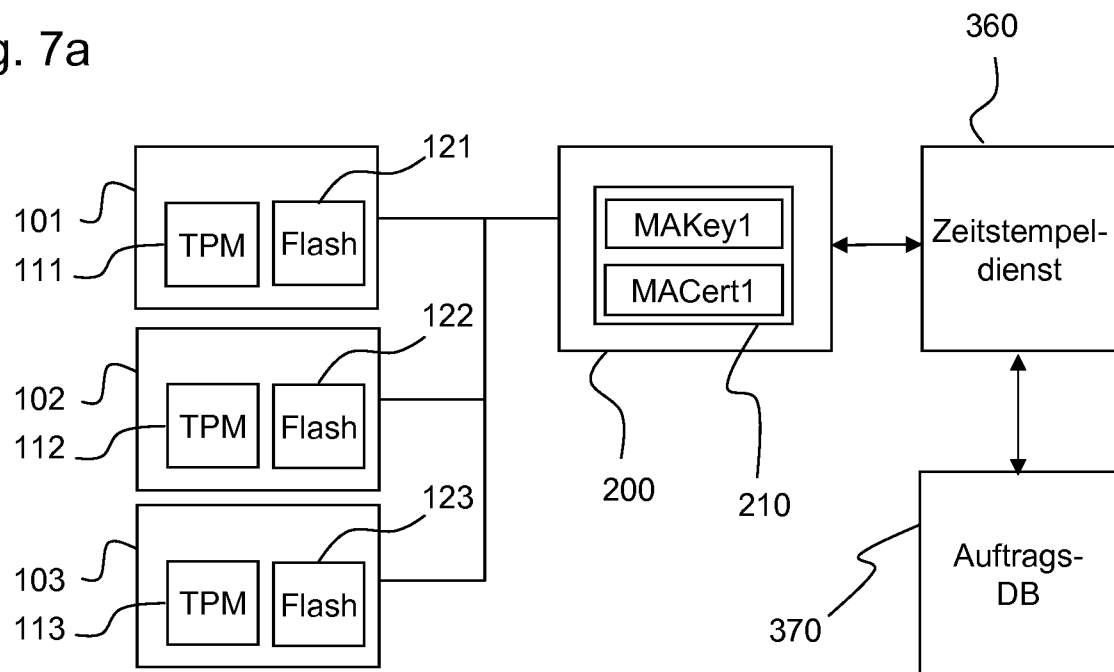


Fig. 7b

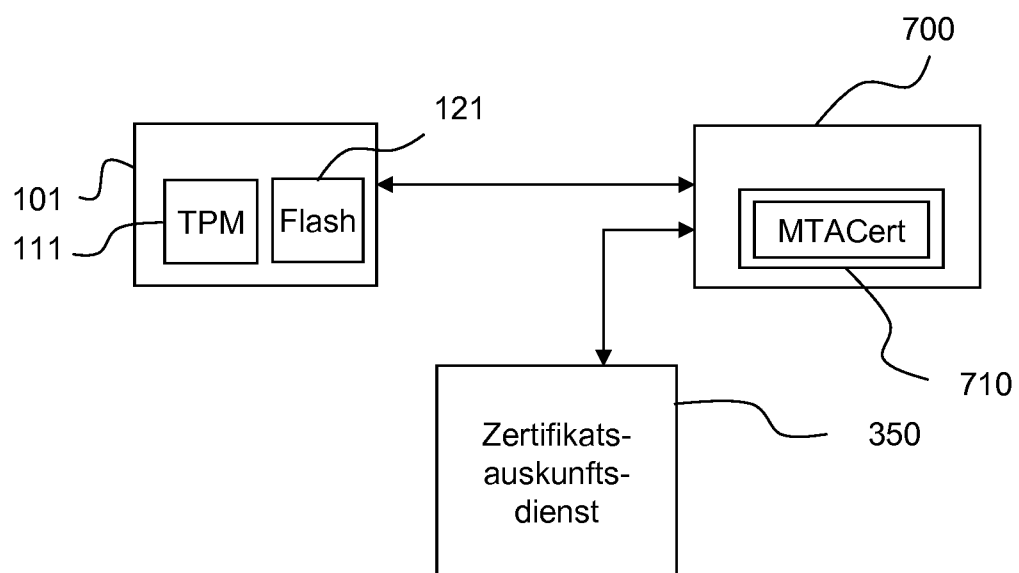


Fig. 8

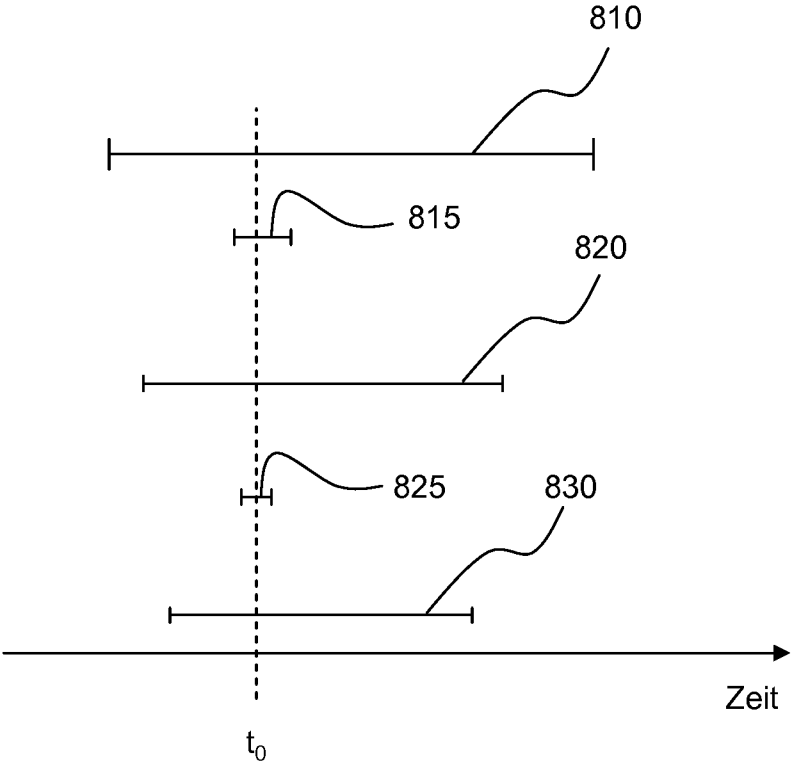


Fig. 9

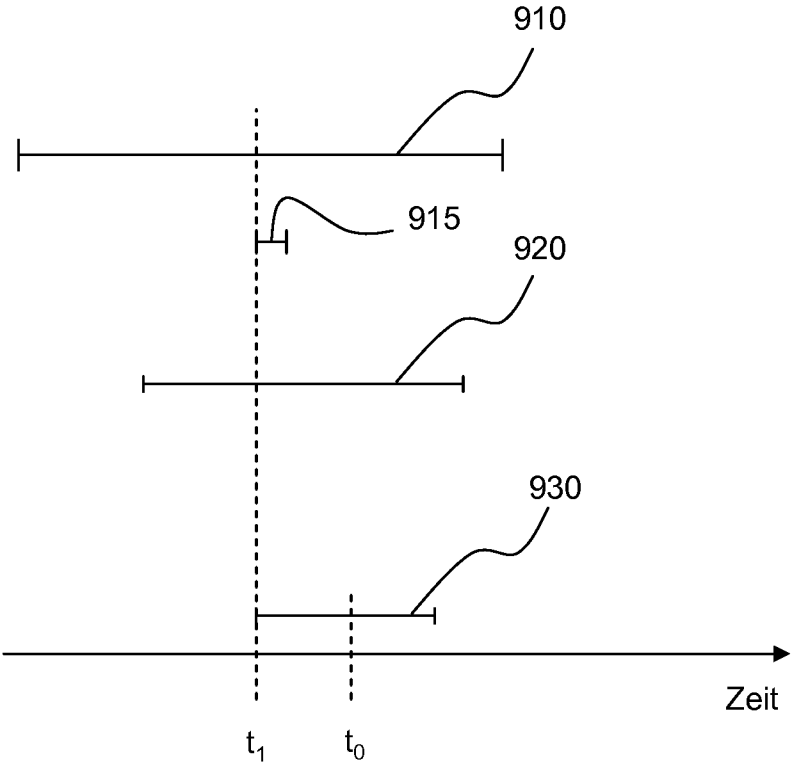


Fig. 10

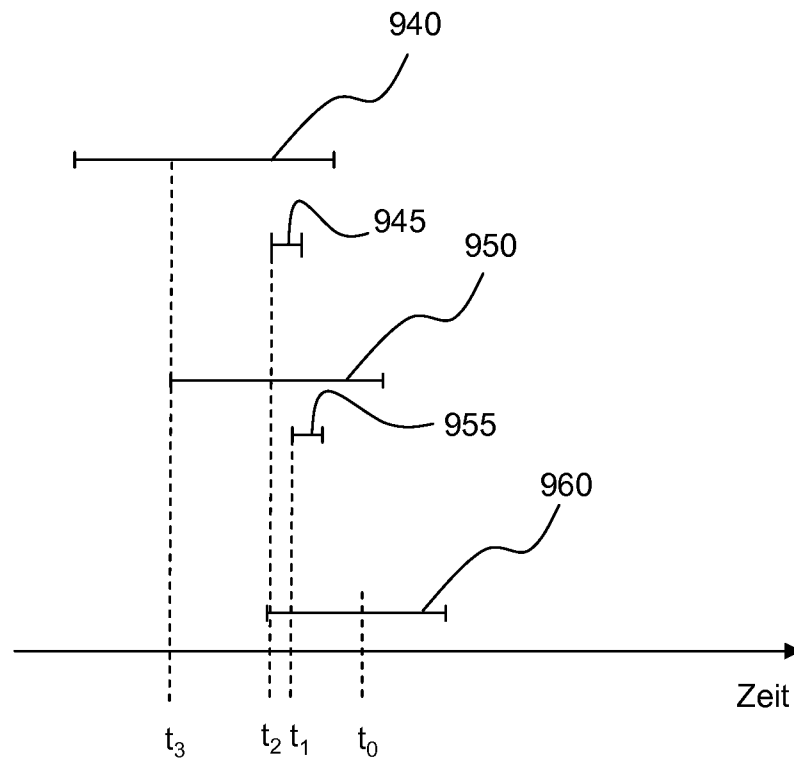
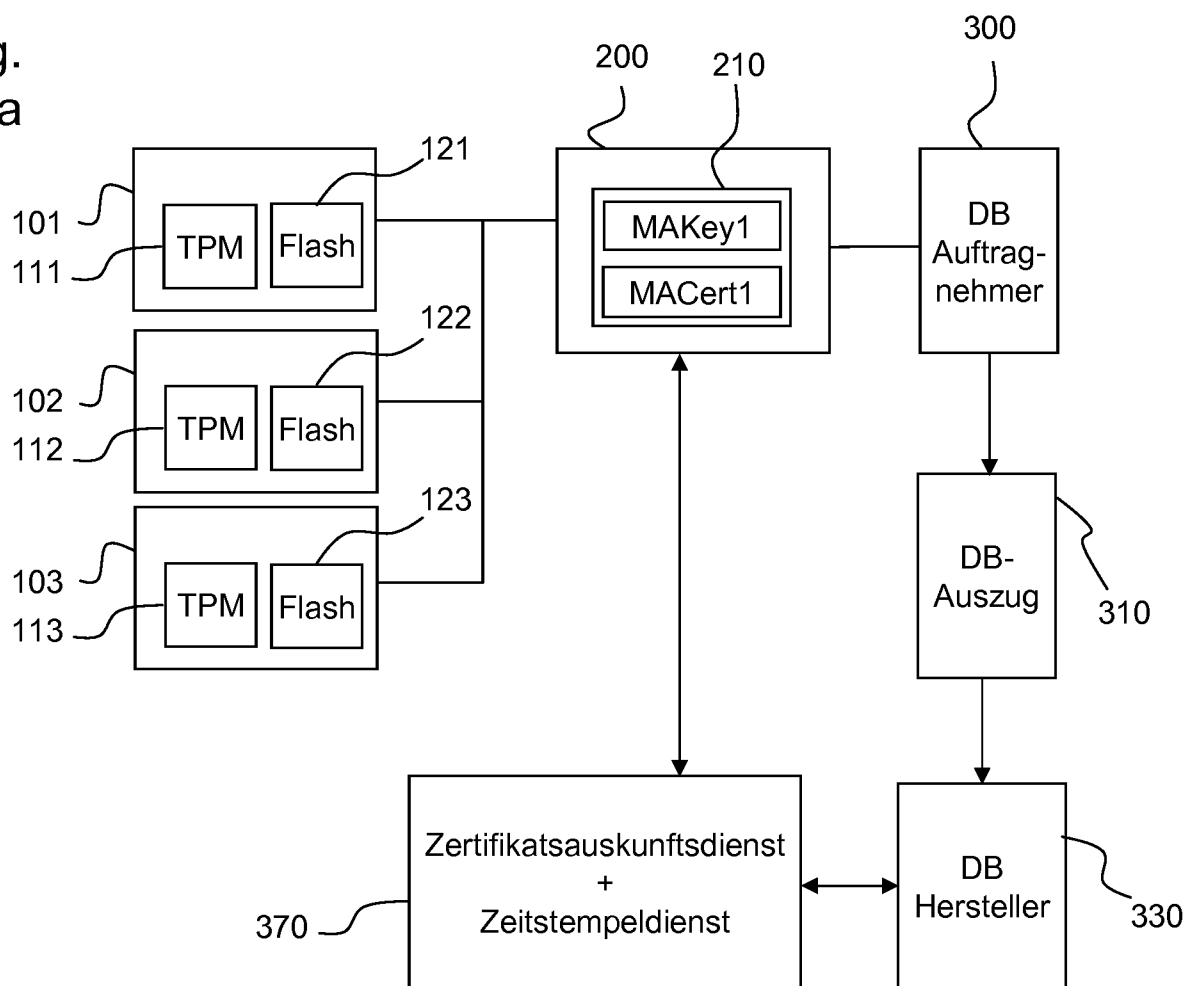
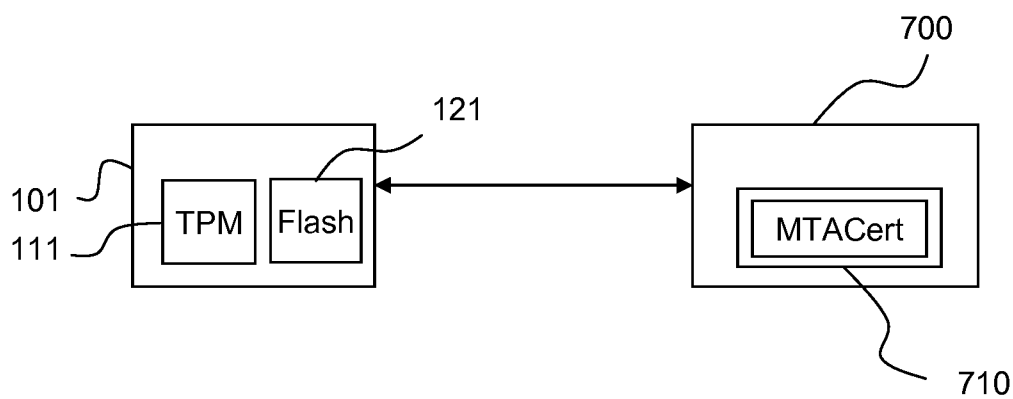


Fig.
11aFig.
11b

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2015/053622

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/32
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 6 389 537 B1 (DAVIS DEREK L [US] ET AL) 14 May 2002 (2002-05-14) column 3, line 16 - column 6, line 20 -----	1-25
Y	CAPKUN S ET AL: "Self-Organized Public-Key Management for Mobile Ad Hoc Networks", TECHNICAL REPORTS IN COMMUNICATIONS SCIENCE OF ECOLEPOLYTECHNIQUE FEDERALE DE LAUSANNE, XX, XX, 28 May 2002 (2002-05-28), pages 1-17, XP002292469, the whole document -----	1-25
A	US 2007/220259 A1 (PAVLICIC MILADIN [US]) 20 September 2007 (2007-09-20) abstract paragraphs [0022] - [0032] ----- -/-	1-25



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

5 May 2015

Date of mailing of the international search report

13/05/2015

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Di Felice, M

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2015/053622

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JIN-BUM HWANG ET AL: "Two Layered PKI Model for Device Authentication in Multi-Domain Home Networks", 2006 IEEE TENTH INTERNATIONAL SYMPOSIUM, IEEE, 28 June 2006 (2006-06-28), pages 1-6, XP010937934, DOI: 10.1109/ISCE.2006.1689451 ISBN: 978-1-4244-0216-8 the whole document	1-25
A	----- US 2013/283042 A1 (XIAO SIHAI [US]) 24 October 2013 (2013-10-24) abstract paragraphs [0047] - [0050] -----	1-25

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2015/053622

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6389537	B1	14-05-2002	AU 4184300 A 10-11-2000
		DE 60015964 D1 23-12-2004	
		DE 60015964 T2 22-12-2005	
		EP 1183582 A1 06-03-2002	
		US 6389537 B1 14-05-2002	
		US 2002040436 A1 04-04-2002	
		WO 0065426 A1 02-11-2000	

US 2007220259	A1	20-09-2007	CN 101395624 A 25-03-2009
		EP 1999696 A2 10-12-2008	
		KR 20080104137 A 01-12-2008	
		US 2007220259 A1 20-09-2007	
		WO 2007106272 A1 20-09-2007	

US 2013283042	A1	24-10-2013	AU 3712300 A 02-01-2001
		US 2002152382 A1 17-10-2002	
		US 2009222574 A1 03-09-2009	
		US 2012023328 A1 26-01-2012	
		US 2013283042 A1 24-10-2013	
		US 2015100786 A1 09-04-2015	
		WO 0077974 A1 21-12-2000	

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES INV. H04L9/32 ADD.		
Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC		
B. RECHERCHIERTE GEBIETE		
Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole) H04L		
Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen		
Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe) EPO-Internal		
C. ALS WESENTLICH ANGESEHENE UNTERLAGEN		
Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	US 6 389 537 B1 (DAVIS DEREK L [US] ET AL) 14. Mai 2002 (2002-05-14) Spalte 3, Zeile 16 - Spalte 6, Zeile 20 -----	1-25
Y	CAPKUN S ET AL: "Self-Organized Public-Key Management for Mobile Ad Hoc Networks", TECHNICAL REPORTS IN COMMUNICATIONS SCIENCE OF ECOLEPOLYTECHNIQUE FEDERALE DE LAUSANNE, XX, XX, 28. Mai 2002 (2002-05-28), Seiten 1-17, XP002292469, das ganze Dokument -----	1-25
A	US 2007/220259 A1 (PAVLICIC MILADIN [US]) 20. September 2007 (2007-09-20) Zusammenfassung Absätze [0022] - [0032] ----- -/-	1-25
☒ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen ☒ Siehe Anhang Patentfamilie		
* Besondere Kategorien von angegebenen Veröffentlichungen : "A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist "E" frühere Anmeldung oder Patent, die bzw. das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist "L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt) "O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht "P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist "T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist "X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden "Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist "&" Veröffentlichung, die Mitglied derselben Patentfamilie ist		
Datum des Abschlusses der internationalen Recherche 5. Mai 2015		Absendedatum des internationalen Recherchenberichts 13/05/2015
Name und Postanschrift der Internationalen Recherchenbehörde Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Bevollmächtigter Bediensteter Di Felice, M

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN		
Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	JIN-BUM HWANG ET AL: "Two Layered PKI Model for Device Authentication in Multi-Domain Home Networks", 2006 IEEE TENTH INTERNATIONAL SYMPOSIUM, IEEE, 28. Juni 2006 (2006-06-28), Seiten 1-6, XP010937934, DOI: 10.1109/ISCE.2006.1689451 ISBN: 978-1-4244-0216-8 das ganze Dokument -----	1-25
A	US 2013/283042 A1 (XIAO SIHAI [US]) 24. Oktober 2013 (2013-10-24) Zusammenfassung Absätze [0047] - [0050] -----	1-25

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP2015/053622

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 6389537	B1	14-05-2002	AU 4184300 A 10-11-2000
		DE 60015964 D1 23-12-2004	
		DE 60015964 T2 22-12-2005	
		EP 1183582 A1 06-03-2002	
		US 6389537 B1 14-05-2002	
		US 2002040436 A1 04-04-2002	
		WO 0065426 A1 02-11-2000	
US 2007220259	A1	20-09-2007	CN 101395624 A 25-03-2009
		EP 1999696 A2 10-12-2008	
		KR 20080104137 A 01-12-2008	
		US 2007220259 A1 20-09-2007	
		WO 2007106272 A1 20-09-2007	
US 2013283042	A1	24-10-2013	AU 3712300 A 02-01-2001
		US 2002152382 A1 17-10-2002	
		US 2009222574 A1 03-09-2009	
		US 2012023328 A1 26-01-2012	
		US 2013283042 A1 24-10-2013	
		US 2015100786 A1 09-04-2015	
		WO 0077974 A1 21-12-2000	