(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
6. August 2009 (06.08.2009)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2009/095143 A1

(51) Internationale Patentklassifikation:
H04L 9/30 (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2008/068361

(22) Internationales Anmeldedatum:
30. Dezember 2008 (30.12.2008)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2008 006 359.2 28. Januar 2008 (28.01.2008) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **SIEMENS AKTIENGESELLSCHAFT** [DE/DE]; Wittelsbacherplatz 2, 80333 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **MEYER, Bernd** [DE/DE]; Sundergaustrasse 137, 81739 München (DE).

(74) Gemeinsamer Vertreter: **SIEMENS AKTIENGESELLSCHAFT**; Postfach 22 16 34, 80506 München (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, 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, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM,

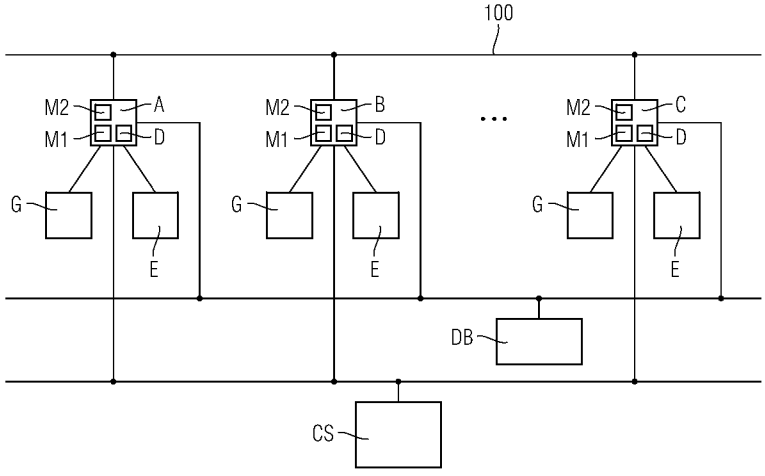
[Fortsetzung auf der nächsten Seite]

WO 2009/095143 A1

(54) **Title:** ASYMMETRICAL CRYPTOSYSTEM

(54) **Bezeichnung:** ASYMMETRISCHES KRYPTOSYSTEM

FIG 1



(57) **Abstract:** An increased degree of security is achieved in asymmetrical cryptosystems by using key pairs comprising private and public keys since the communication partners must not know a common, secret key. In many applications, it is therefore necessary to store the key pair together with a digital signature on the appropriate hardware. However, when asymmetrical cryptographic methods are used in systems with a limited storage capacity, for example smart cards, RFIDs or embedded systems, as little storage space as possible should always be required. For this purpose, the invention proposes a solution in which it is no longer necessary to store the public key.

(57) **Zusammenfassung:** In asymmetrischen Kryptosystemen wird durch die Verwendung von Schlüsselpaaren aus privaten und öffentlichen Schlüsseln ein erhöhtes Maß an Sicherheit erzielt, da die Kommunikationspartner keinen gemeinsamen, geheimen Schlüssel kennen müssen. In vielen Anwendungen ist

[Fortsetzung auf der nächsten Seite]

ST, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:
— *mit internationalem Recherchenbericht*

es daher erforderlich, dass das Schlüsselpaar zusammen mit einer digitalen Signatur auf der entsprechenden Hardware gespeichert sein müssen. Für Anwendungen von asymmetrischen Kryptographieverfahren auf Systemen mit begrenzter Speicherplatzkapazität, wie beispielsweise Smartcards, RFIDs oder Embedded Systems, besteht jedoch die Anforderung, dass stets möglichst wenig Speicherplatz benötigt werden sollte. Die Erfindung schlägt hierzu eine Lösung vor, bei der die Speicherung des öffentlichen Schlüssels nicht mehr notwendig ist.

Beschreibung

Asymmetrisches Kryptosystem

Verfahren zur Bereitstellung eines öffentlichen Schlüssels für ein asymmetrisches Kryptosystem und ein asymmetrisches Kryptosystem.

Asymmetrische Kryptosysteme gewährleisten durch die Einrichtung von Schlüsselpaaren aus privatem und öffentlichem Schlüssel ein erhöhtes Maß an Sicherheit. So ist es für einen Angreifer nahezu unmöglich, in endlicher Zeit ohne den privaten Schlüssel die mit dem öffentlichem Schlüssel verschlüsselte Nachricht zu entschlüsseln. Übliche Kryptosysteme basieren auf einer Verschlüsselung, die in polynomieller Zeit durchführbar, jedoch nur in sub-exponentieller oder exponentieller Zeit relativ zur Länge der Schlüssel in Bits invertierbar ist. Bei auf elliptischen Kurven basierenden Systemen werden heute beispielsweise Schlüssellängen von N = 160 bis 300 Bits verwendet. Bei denen auf RSA Algorithmen basierenden Systemen sind dazu Schlüssellängen von N = 1024 bis 4096 Bits für ein etwa gleiches Sicherheitsniveau anzusetzen.

Allerdings muss bei asymmetrischen Kryptographieverfahren sichergestellt werden, dass der öffentliche Schlüssel zur Kommunikation mit einem anderen Kommunikationsteilnehmer tatsächlich von diesem stammt und somit authentisch ist. Diese Schwachstelle wird beispielsweise bei dem sogenannten Man-in-the-Middle Angriff genutzt, bei dem sich ein Angreifer als berechtigter Adressat ausgibt. Hierzu generiert er selbst ein Paar aus einem öffentlichen und einem privaten Schlüssel. Den öffentlichen Schlüssel übermittelt er dem Absender und suggeriert ihm, dass dieser öffentliche Schlüssel von dem berechtigten Adressaten stammt. Anschließend entschlüsselt der Mittelsmann die Nachricht mit seinem eigenen privaten Schlüssel, verschlüsselt die Nachricht mit dem richtigen

öffentlichen Schlüssel des Adressaten wieder und sendet sie weiter. Auf diese Weise kann der Angreifer unbemerkt von den eigentlichen Kommunikationspartnern deren geheime Nachrichten mitlesen.

Daher wird versucht, beispielsweise mit dem Einsatz von zentralen Zertifizierungsstellen oder durch Etablierung eines Web-of-Trust eine vertrauenswürdige Instanz zu schaffen, durch die die Authentizität von öffentlichen Schlüsseln gewährleistet werden soll.

Dieses Signieren eines öffentlichen Schlüssels einer Person zusammen mit dessen persönlichen Daten, zum Beispiel dem Namen, der Email Adresse, etc. kann wiederum unter Verwendung von asymmetrischer Kryptographie geschehen. Im Wesentlichen errechnet dabei die Zertifizierungsstelle eine Prüfsumme der Kombination aus dem öffentlichen Schlüssel einer Person und deren persönlichen Daten. Durch Anwenden eines privaten Schlüssels der Zertifizierungsstelle auf die Prüfsumme wird eine digitale Signatur erzeugt. Da der öffentliche Schlüssel der Zertifizierungsstelle frei zugänglich gemacht wird, ist es jedermann möglich, die digitale Signatur zu prüfen. Der private Schlüssel der Zertifizierungsstelle ist jedoch nicht öffentlich zugänglich, so dass niemand Daten so signieren kann, dass sie mit dem öffentlichen Schlüssel der Zertifizierungsstelle wieder als gültig verifiziert werden können.

In vielen Anwendungen ist es daher erforderlich, dass das Schlüsselpaar aus privatem und öffentlichem Schlüssel, sowie die digitale Signatur auf der benötigten Hardware gespeichert sein müssen. Für eine sichere Kommunikation übersendet dann der Adressat dem Absender seinen öffentlichen Schlüssel und die dazugehörige digitale Signatur. Für Anwendungen von asymmetrischen Kryptographieverfahren auf Systemen mit begrenzter Speicherplatzkapazität, wie beispielsweise Smartcards, RFIDs oder Embedded Systems, besteht jedoch die

Anforderung, dass stets möglichst wenig Speicherplatz verwendet werden sollte.

Daher ist die Aufgabe der vorliegenden Erfindung, ein asymmetrisches Kryptosystem und Kryptographieverfahren anzugeben, welches bei gleichem Sicherheitsniveau möglichst wenig Speicherplatz beanspruchen.

Erfindungsgemäß wird dieser Aufgabe durch ein Verfahren und ein System mit den Merkmalen der Ansprüche 1 und 6 gelöst. Vorteilhafte Weiterbildungen der Erfindung sind in den abhängigen Ansprüchen angegeben.

Erfindungsgemäß ist in einem Verfahren zur Bereitstellung eines öffentlichen Schlüssels für ein asymmetrisches Kryptosystem mit einem Schlüsselinhaber und einem Schlüsselanforderer dem Schlüsselinhaber ein Schlüsselpaar mit einem privaten und mindestens einem öffentlichem Schlüssel zugeordnet. Weiterhin ist dem Schlüsselpaar eine digitale Signatur zur Authentifizierung des öffentlichen Schlüssels zugeordnet. Gemäß dem erfindungsgemäßen Verfahren sind der private Schlüssel und die digitale Signatur gespeichert. Der öffentliche Schlüssel wird auf Anfrage des Schlüsselanforderers aus dem privaten Schlüssel abgeleitet. Schließlich werden der abgeleitete öffentliche Schlüssel und die digitale Signatur dem Schlüsselanforderer bereitgestellt. Dies hat den Vorteil, dass die üblicherweise in Zertifikaten enthaltene Information reduziert wird und damit der Speicherbedarf auf Seiten des Schlüsselinhabers für die Zertifikate reduziert wird. Üblicherweise umfasst ein Zertifikat eines Schlüsselinhabers den öffentlichen Schlüssel, eine digitale Signatur einer Zertifizierungsstelle, sowie weitere Angaben zur Identifizierung der Person des Schlüsselinhabers und/oder Attribute, welche Eigenschaften und/oder Rechte des zugehörigen Schlüsselpaares und Schlüsselinhabers charakterisieren.

Gemäß einer vorteilhaften Ausgestaltung der vorliegenden Erfindung erfolgt die Ableitung des öffentlichen Schlüssels durch hardwaretechnisch gesicherte Maßnahmen.

Zur hardwaretechnischen Absicherung des Verfahrens ist in dieser Erfindung ohne Ausschluss der Allgemeinheit dieses Begriffs ein Koprozessor, insbesondere ein Krypto-Koprozessor zu verstehen. Dieser verfügt über einen eingeschränkten Befehlssatz und ist hardwaretechnisch derart geschützt, dass durch Messungen nahezu nicht erkennbar ist, ob gleichwertige oder ungleichwertige Operationen in dem Koprozessor durchgeführt werden. Insbesondere wird dadurch die praktische Durchführbarkeit von sogenannten Seitenkanalangriffen verhindert.

Gemäß einer weiteren vorteilhaften Ausgestaltung der Erfindung erfolgt die Ableitung des öffentlichen Schlüssels durch Exponentiation oder Skalarmultiplikation eines gegebenen Gruppenelements einer endlichen Gruppe mit dem privaten Schlüssel.

Das erfindungsgemäße asymmetrische Kryptosystem weist mindestens ein anwenderspezifisches Schlüsselpaar mit einem privaten und mindestens einem öffentlichem Schlüssel, sowie eine digitale Signatur zur Authentifizierung des öffentlichen Schlüssels auf. Auf einer Speichervorrichtung des Systems sind der private Schlüssel und die digitale Signatur gespeichert. Durch eine Rechenvorrichtung des Systems wird der öffentliche Schlüssel auf Anfrage aus dem privaten Schlüssel abgeleitet. Schließlich wird durch eine Kommunikationsvorrichtung des Systems der abgeleitete, öffentliche Schlüssel bereitgestellt.

Nachfolgend wird die Erfindung anhand von Ausführungsbeispielen und den Figuren näher erläutert. In den Figuren zeigen:

Figur 1 ein Blockdiagramm eines Ausführungsbeispiel der vorliegenden Erfindung,

Figur 2 ein Flussdiagramm zur Erläuterung einer Ausführungsform des erfindungsgemäßen Verfahrens,

Figur 3 ein Flussdiagramm zur Illustration einer Kommunikation zwischen zwei Teilnehmern, welche sich des erfindungsgemäßen Verfahrens und eines Netzwerks nach Figur 1 bedienen.

In Figur 1 ist eine beispielhafte Topologie eines Netzwerkes nach einem Ausführungsbeispiel der vorliegenden Erfindung gezeigt. Eine Anwenderstelle A ist über eine Datenleitung 100 mit einer Mehrzahl weiterer Anwenderstellen B, C verbunden. Die Datenleitung kann durch ein internes Netzwerk oder ein externes Netzwerk, wie das Internet, bereitgestellt werden. Die Datenübertragung kann drahtgebunden, drahtlos oder optisch erfolgen. Jede der Anwenderschnittstellen A, B, C weist eine Eingabeeinrichtung E auf. Diese kann in vielfältigsten Weisen ausgeführt sein und dient zum Erstellen von Botschaften, Eingeben von persönlichen Daten etc. In dem in Figur 1 dargestellten Ausführungsbeispiel ist jede Anwenderschnittstelle A, B, C mit einem individuellen Schlüsselgenerator G verbunden. Dieser Schlüsselgenerator kann per Software auf einer Rechnereinheit oder durch einen hardwarebasierten Schlüsselgenerator realisiert werden. Ferner kann anstelle des dargestellten Ausführungsbeispiels auch ein zentraler Schlüsselgenerator G für eine Vielzahl von Anwenderschnittstellen A, B, C bereitgestellt werden. Der Schlüsselgenerator G erstellt einen privaten Schlüssel PSA individuell für eine Anwenderschnittstelle A und speichert diesen lokal bei der Anwenderschnittstelle A in einem ersten Speicher M1 ab. Zusätzlich erstellt der Schlüsselgenerator G einen öffentlichen Schlüssel OSA basierend auf dem privaten Schlüssel PSA.

Die Anwenderschnittstelle A fordert nun den Bediener auf, persönliche Daten anzugeben. Diese beinhalten zum Beispiel den Vornamen, den Nachnamen, einen Rufnamen, die Email Adresse, eine postalische Adresse, eine Telefonnummer, eine Kontonummer oder weitere persönliche Kennzeichen des Anwenders. Auf Grundlage dieser Angaben und des öffentlichen Schlüssels OSA wird durch eine Zertifizierungsstelle CS eine digitale Signatur ZA erstellt, welche lokal in einem zweiten Speicher M2 der Anwenderschnittstelle A gespeichert wird.

Anhand des Flussdiagramm in Figur 2 wird beispielhaft der Verfahrensablauf zur Ermittlung der digitalen Signatur erläutert. In diesem Beispiel wird nur der Name N des Anwenders von der Anwenderschnittstelle abgefragt. Dieser heiße Frank Mustermann (S2).

Die Anwenderschnittstelle oder eine darin befindliche Datenverarbeitungseinrichtung D wendet eine vorbestimmte Hashfunktion h auf den Namen N an (S3). Die Hashfunktion h ist in einem Protokoll für die Netzwerkkommunikation festgelegt. Beispielsweise kann dieses der Message Digest Algorithm 5 (md5) sein. Dieser angewendet auf den Namen Frank Mustermann ergibt 639d 0c04 06d1 f526 59c2 509b 8c6e 6550 in hexadezimaler Darstellung. Die Anwendung der md5 Hashfunktion auf einen ähnlich klingenden Namen, zum Beispiel Bernd Mustermann ergibt einen vollständig anderen Hashwert H, nämlich 7df4 c6fc 3e3c 4a61 0dfa 687a 40b7 2711. Eine der wesentlichen Eigenschaften der Hashfunktion h ist, dass bei geringen Änderungen des Eingabewertes, in diesem Fall des Namens N, ein deutlich verschiedener Hashwert H bestimmt wird. Eine weitere wesentliche Eigenschaft der Hashfunktion h ist, das sie nur unter verhältnismäßig hohem Aufwand umkehrbar ist. Weitere bekannte Hashfunktionen sind der SHA-1 Algorithmus (Secure Hash Algorithm) und der SHA-256 Algorithmus.

Die Anwenderschnittstelle A übermittelt den Hashwert H zusammen mit dem öffentlichen Schlüssel des Anwenders OSA an eine zentrale Zertifizierungsstelle CS (S4). Die Zertifizierungsstelle CS hat bereits ihren öffentlichen Schlüssel OSCS und ihren privaten Schlüssel PSCS erstellt (S5). Zunächst fügt die Zertifizierungsstelle CS den übermittelten Hashwert H und den übermittelten öffentlichen Schlüssel OSA zu einem Datum KA zusammen (S6). Danach signiert sie das Datum KA oder die Kombination KA mit ihrem privaten Schlüssel PSCS (S7), um die Signatur ZA zu generieren. Üblicherweise erfolgt das Signieren nur dann, wenn der Anwender sich gegenüber der Zertifizierungsstelle CS eindeutig ausweisen kann, zum Beispiel durch persönliche Anwesenheit in Kombination mit einem Personalausweis.

Abschließend werden der Hashwert H und die erstellte Signatur ZA von der Zertifizierungsstelle CS an den Anwender A übermittelt und von diesem lokal in einem zweiten Speicher M2 gespeichert.

Unter Verweis auf das Flussdiagramm in Figur 3 wird nachfolgend eine Übermittlung einer Botschaft T von einem Anwender B an den vorherigen Anwender A beschrieben. Zunächst generiert der Anwender B seinen privaten und seinen öffentlichen Schlüssel PSB, OSB und verfasst die Botschaft T. Nachfolgend chiffriert er die Botschaft T mit einem Chiffrierschlüssel C mit einem der vielen bekannten Verschlüsselungsverfahren (S10 - S12).

Der Anwender B kennt den Namen N des Anwenders A und möchte nun mit ihm über einen verschlüsselten Kanal kommunizieren. Dazu benötigt er zunächst den öffentlichen Schlüssel OSA des Anwenders A und muss auch nachfolgend sicherstellen, dass der von ihm erhaltene öffentliche Schlüssel OSA wirklich dem Anwender A zugeordnet ist. Auf Anfrage des Anwenders B leitet der Anwender A aus seinem privaten Schlüssel PSA seinen öffentlichen Schlüssel OSA ab und übermittelt seinen

abgeleiteten öffentlichen Schlüssel OSA zusammen mit der gespeicherten Signatur ZA und dem zugehörigen, gespeicherten Hashwert H an den Anwender B (S13, S14). Zusätzlich bezieht der Anwender B den öffentlichen Schlüssel OSCS der Zertifizierungsstelle CS (S15, S16).

Aus der Signatur ZA wird mit Hilfe des öffentlichen Schlüssels OSCS der Zertifizierungsstelle CS die Authentizität der Kombination KA geprüft (S17). Der Kombinationswert KA wird für einen nachfolgenden Vergleichsschritt gespeichert. In einem nachfolgend, parallel oder zuvor ausgeführten Schritt wird aus dem bekannten Namen N unter Verwendung der bekannten Hashfunktion h der zu testende Hashwert H_t bestimmt (S18). Dieser kann mit dem von der Zertifizierungsstelle bezogenen Hashwert H verglichen werden. Stimmen die beiden Hashwerte H und Ht überein, so ist das Zertifikat ZA der gewünschten Person -also dem Anwender A- zugeordnet. Nachfolgend wird der Hashwert Ht mit dem bezogenen öffentlichen Schlüssel OSA zu einer zu testenden Kombination Kt kombiniert. Diese zu testende Kombination Kt wird mit der in Schritt S17 bestimmten Kombination verglichen (S20). Bei Übereinstimmung der beiden Kombinationen KA, Kt ist der öffentliche Schlüssel OSA als Schlüssel des Anwenders A verifiziert (S21).

Nachfolgend kann der Anwender B den Chiffrierschlüssel mit dem öffentlichen Schlüssel OSA des Anwenders A zu einem verschlüsselten Chiffrierschlüssel Cg verschlüsseln (S22). Abschließend erfolgt eine Übertragung der chiffrierten Botschaft Tg und des verschlüsselten Chiffrierschlüssels Cg (S23) an den Anwender A.

Für den Fachmann ist ersichtlich, dass vielfältige Verfahrensschritte in anderer Reihenfolge ausgeführt werden können, als sie in dem vorstehenden Ausführungsbeispiel dargestellt sind.

Das erfindungsgemäße Verfahren ist besonders vorteilhaft anwendbar bei Systemen basierend auf Smartcards, embedded Systems oder RFIDs mit asymmetrischem Schlüsselmanagement. Diese werden beispielsweise zur Zugangskontrolle oder in Systemen zum Schutz vor Plagiaten eingesetzt.

Die Sicherheit eines exemplarisch dargestellten Kryptosystems mit asymmetrischem Schlüsselmanagement beruht auf der Schwierigkeit der Berechnung diskreter Logarithmen in endlichen abelschen Gruppen. Beispiele für kryptographische Verfahren, die diese Techniken verwenden, sind ElGamal, DSA, GDSA, DH, sowie die entsprechenden Varianten dieser Verfahren, die auf Punktgruppen elliptischer oder hyperelliptischer Kurven über endlichen Körpern beruhen.

Im folgenden Ausführungsbeispiel wird die Ableitung eines öffentlichen Schlüssels aus einem privaten Schlüssel für derartige Systeme beispielhaft dargestellt. Demgemäß enthält die kryptographische Sicherheitshardware auf einem RFID einen privaten Schlüssel. Bei multiplikativer Gruppendarstellung berechnet sie eine Exponentiation eines als Input gegebenen Gruppenelements mit dem privaten Schlüssel und gibt das Ergebnis dieser Exponentiation als Output zurück. Bei additiver Gruppendarstellung wird entsprechend eine Skalarmultiplikation eines als Input gegebenen Gruppenelements mit dem privaten Schlüssel als Skalar berechnet und das Ergebnis dieser Skalarmultiplikation als Output zurückgegeben.

Die Erzeugung eines Schlüsselpaares, bestehend aus geheimem und öffentlichem Schlüssel, wird folgendermaßen durchgeführt: Das System wählt eine zufällige Zahl modulo der Ordnung einer von einem als Systemparameter vorgegebenen Basiselement der Gruppe erzeugten zyklischen Untergruppe als geheimen Schlüssel. Der öffentliche Schlüssel wird durch Exponentiation (beziehungsweise Skalarmultiplikation) des Basiselements mit dem geheimen Schlüssel als Exponent

(beziehungsweise als Skalar) erhalten. Als letzter Schritt der Schlüsselerzeugung wird der auf diese Weise erzeugte öffentliche Schlüssel von einer Zertifizierungsstelle (gegebenenfalls zusammen mit weiteren Attributen) signiert und bildet das Zertifikat. Das zur Schlüsselerzeugung verwendete Basiselement ist dabei ein öffentlich bekannter Systemparamter.

Zur Ermittlung des öffentlichen Schlüssels aus dem gespeicherten privaten Schlüssel wird nun analog zur ursprünglichen Erzeugung des öffentlichen Schlüssels vorgegangen: Das System liest den gespeicherten geheimen Schlüssel aus und berechnet eine Exponentiation (beziehungsweise Skalarmultiplikation) des öffentlich bekannten Basiselements mit dem geheimen Schlüssel als Exponent (beziehungsweise als Skalar). Auf diese Weise wird der gleiche Wert für den öffentlichen Schlüssel ermittelt wie bei der ursprünglichen Schlüsselerzeugung.

Der öffentliche Schlüssel wird durch Exponentiation, bzw. Skalarmultiplikation, des Basiselements mit dem privaten Schlüssel als Exponent, bzw. als Skalar, erhalten. Auf diese Weise wird der öffentliche Schlüssel aus dem privaten Schlüssel abgeleitet und bei Bedarf on-the-fly berechnet.

Bei einer Anfrage durch ein Host-System wird der öffentliche Schlüssel entsprechend ermittelt. Nach Erhalt des ermittelten, öffentlichen Schlüssels und der zugehörigen, gespeicherten Signatur prüft das Host-System anhand der Signatur, ob das erhaltene Schlüsselmaterial authentisch ist.

Im beschriebenen Szenario wird der öffentliche Schlüssel nicht in der Sicherheitshardware gespeichert. Es reicht aus, den privaten Schlüssel, gegebenenfalls die Schlüsselattribute und die von der Zertifizierungsstelle erzeugte Signatur zu speichern.

Damit ist es zum Aufbau einer Public-Key Infrastruktur ausreichend, wenn das Hardware-Modul lediglich seinen privaten Schlüssel und die Authentisierungsinformationen seines Zertifikats speichert. Bei Bedarf kann die Hardware mit Hilfe des gespeicherten privaten Schlüssels den öffentlichen Schlüssel selbstständig ableiten, mit der gespeicherten Authentisierungsinformation vervollständigen und auf diese Weise ihr Zertifikat rekonstruieren und einem Kommunikationspartner mitteilen. Da der öffentliche Schlüssel nicht mehr im Hardware-Modul gespeichert werden muss, reduziert sich der für das Schlüsselmaterial benötigte Speicherbedarf.

Durch die Anwendung einer geeigneten Sicherheitshardware, welche erstens den geheimen Schlüssel für Berechnungen zumindest indirekt verfügbar macht ohne seine Sicherheit zu gefährden und welche zweitens sichere Berechnungen unter Verwendung des geheimen Schlüssels ermöglicht, ist ein solches Verfahren ohne Sicherheitseinbußen einzusetzen.

Obwohl die vorliegende Erfindung anhand eines bevorzugten Ausführungsbeispiels beschrieben wurde, ist dem Fachmann ersichtlich, dass vielfältige Änderungen daran vorgenommen werden können, die dennoch im Umfang der Erfindung nach den Patentansprüchen liegen.

Patentansprüche

1. Verfahren zur Bereitstellung eines öffentlichen Schlüssels für ein asymmetrisches Kryptosystem, mit einem Schlüsselinhaber und einem Schlüsselanforderer, bei dem
- dem Schlüsselinhaber ein Schlüsselpaar mit einem privaten und mindestens einem öffentlichen Schlüssel zugeordnet ist,
- dem Schlüsselpaar eine digitale Signatur zur Authentifizierung des öffentlichen Schlüssels zugeordnet ist,
dadurch gekennzeichnet, dass
- der private Schlüssel und die digitale Signatur gespeichert sind,
- der öffentliche Schlüssel auf Anfrage des Schlüsselanforderers aus dem privaten Schlüssel abgeleitet wird,
- der abgeleitete öffentliche Schlüssel und die digitale Signatur dem Schlüsselanforderer bereitgestellt werden.

2. Verfahren nach Anspruch 1, wobei
der öffentliche Schlüssel durch den Schlüsselinhaber nicht gespeichert wird.

3. Verfahren nach Anspruch 1 oder 2, wobei
dem Schlüsselinhaber zusätzlich weitere Schlüsselattribute zugeordnet sind und dem Schlüsselanforderer bereitgestellt werden.

4. Verfahren nach Anspruch 1 oder 2, wobei
die Ableitung des öffentlichen Schlüssels hardwaretechnisch gesichert erfolgt.

5. Verfahren nach Anspruch 1 oder 2, wobei
die Ableitung des öffentlichen Schlüssels durch Exponentiation oder Skalarmultiplikation eines gegebenen Gruppenelements einer endlichen Gruppe mit dem privaten Schlüssel erfolgt.

6. Asymmetrisches Kryptosystem, aufweisend
- mindestens ein anwenderspezifisches Schlüsselpaar mit einem privaten und mindestens einem öffentlichen Schlüssel,
- eine digitale Signatur zur Authentifizierung des öffentlichen Schlüssels,
dadurch gekennzeichnet, dass
- auf einer Speichervorrichtung der private Schlüssel und die digitale Signatur gespeichert sind,
- durch eine Rechenvorrichtung der öffentliche Schlüssel auf Anfrage aus dem privaten Schlüssel abgeleitet wird,
- durch eine Kommunikationsvorrichtung der abgeleitete öffentliche Schlüssel bereitgestellt wird.

7. Kryptosystem nach Anspruch 6, wobei
- die Rechenvorrichtung hardwaretechnisch für eine sichere Datenverarbeitung ausgestaltet ist.

FIG 1

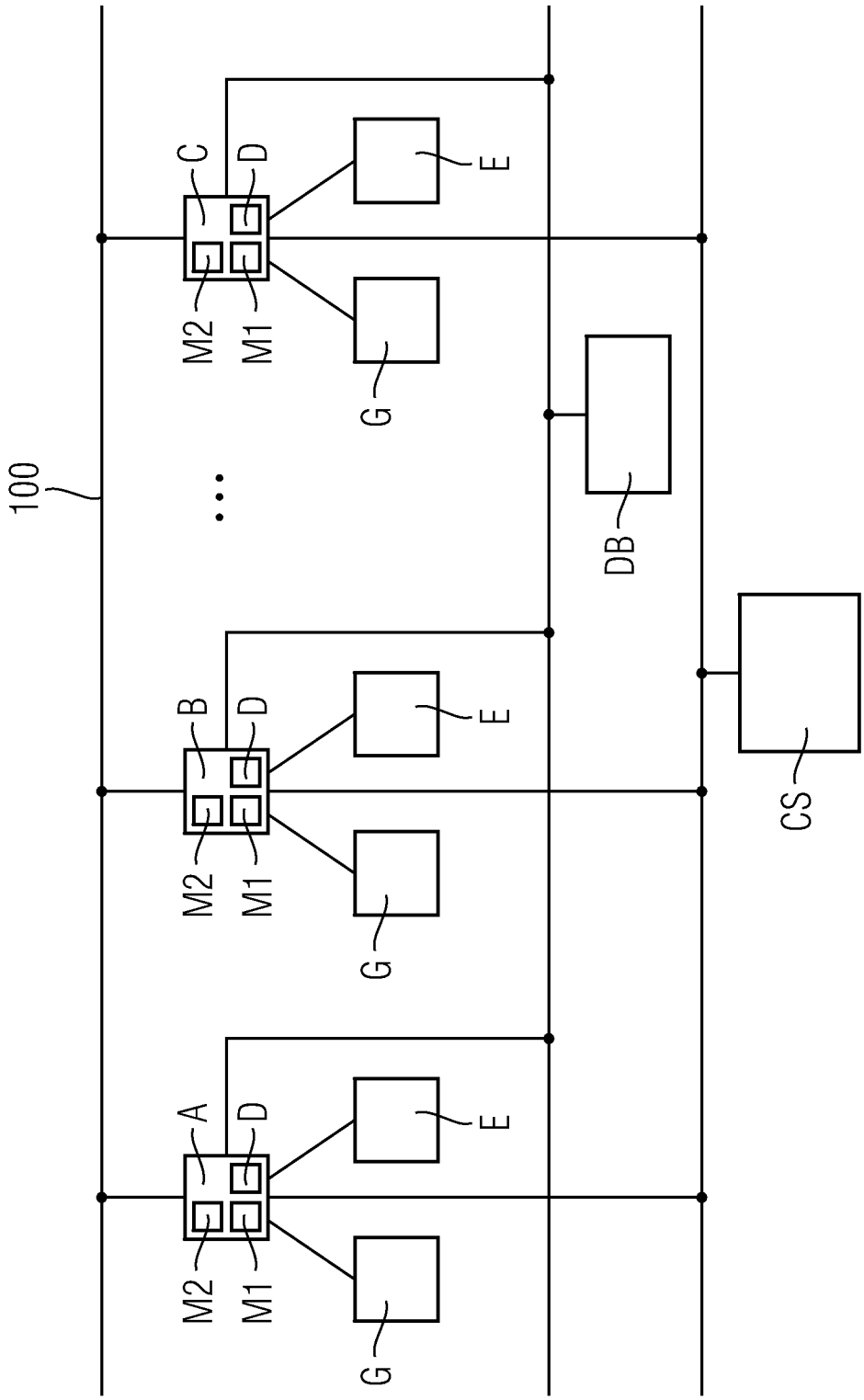


FIG 2

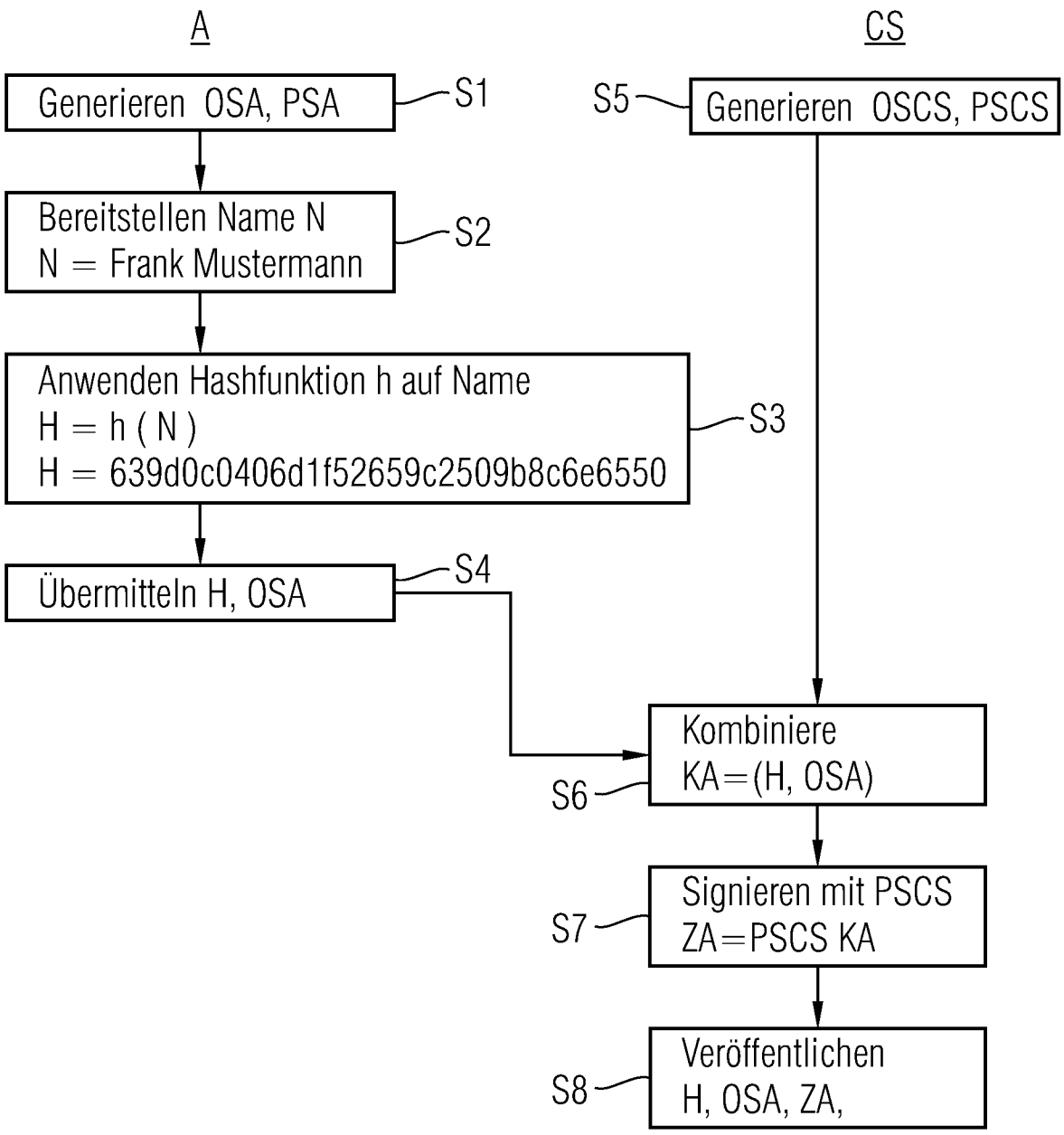
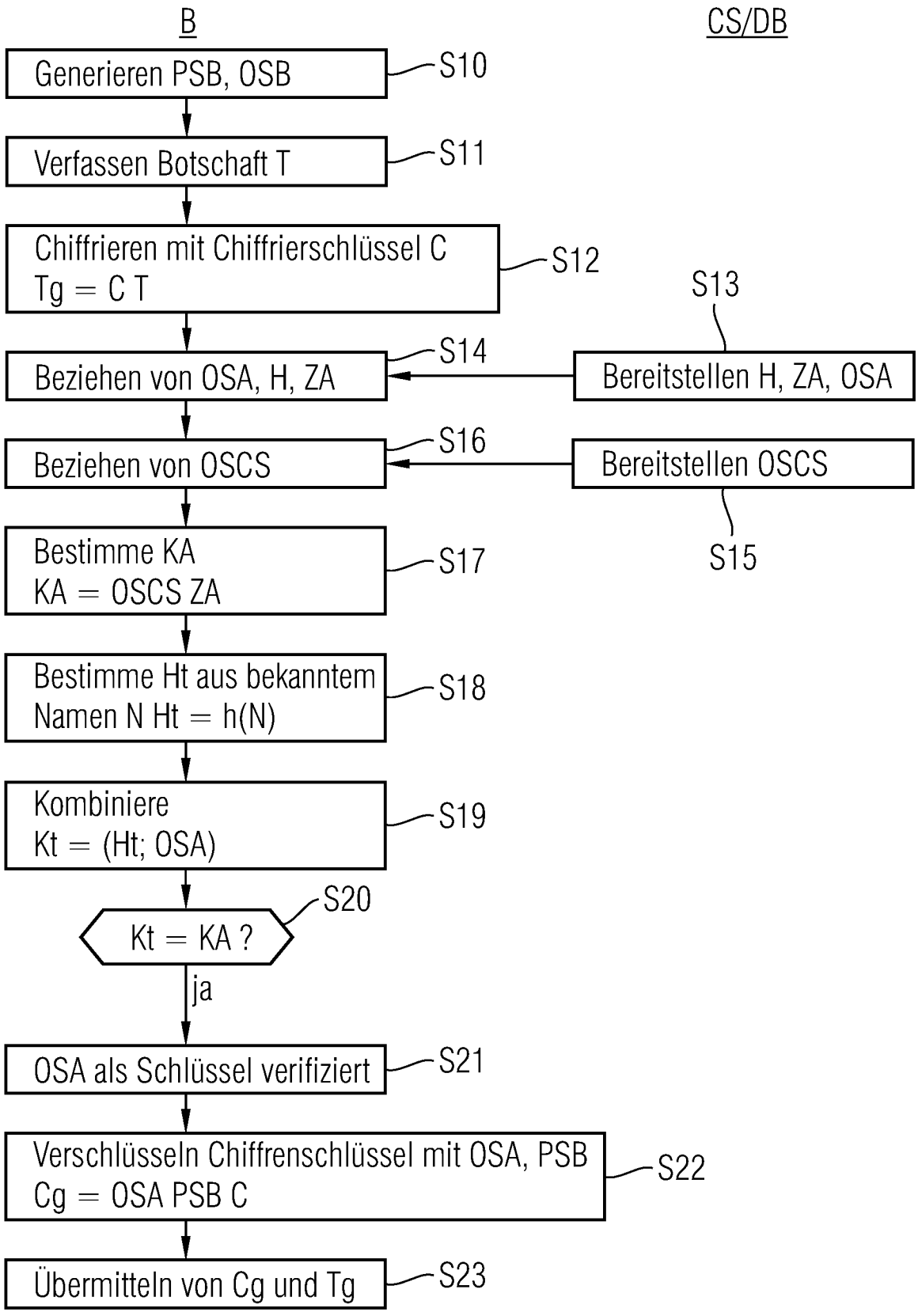

A
CS
Generieren OSA, PSA
S1
S5
Generieren OSCS, PSCS
Bereitstellen Name N
N = Frank Mustermann
S2
Anwenden Hashfunktion h auf Name
H = h (N)
H = 639d0c0406d1f52659c2509b8c6e6550
S3
Übermitteln H, OSA
S4
Kombiniere
KA=(H, OSA)
S6
Signieren mit PSCS
ZA=PSCS KA
S7
Veröffentlichen
H, OSA, ZA,
S8

FIG 3


B
CS/DB
Generieren PSB, OSB
S10
Verfassen Botschaft T
S11
Chiffrieren mit Chiffrierschlüssel C
Tg = C T
S12
S13
Beziehen von OSA, H, ZA
S14
Bereitstellen H, ZA, OSA
Beziehen von OSCS
S16
Bereitstellen OSCS
S15
Bestimme KA
KA = OSCS ZA
S17
Bestimme Ht aus bekanntem
Namen N Ht = h(N)
S18
Kombiniere
Kt = (Ht; OSA)
S19
S20
Kt = KA ?
ja
OSA als Schlüssel verifiziert
S21
Verschlüsseln Chiffrenschlüssel mit OSA, PSB
Cg = OSA PSB C
S22
Übermitteln von Cg und Tg
S23

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2008/068361

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/30

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 G07F

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 practical, 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.
X	GB 2 434 950 A (HEWLETT PACKARD DEVELOPMENT CO [US]) 8 August 2007 (2007-08-08) page 3, lines 22-27 page 8, line 3 - page 9, line 5; figure 2	1-7
A	WO 2006/122433 A (CERTICOM CORP [CA]; VANSTONE SCOTT A [CA]; BROWN DANIEL R L [CA]) 23 November 2006 (2006-11-23) paragraphs [0014], [0015], [0022], [0023]	1-7
A	US 2006/153364 A1 (BEESON CURTIS L [US]) 13 July 2006 (2006-07-13) paragraph [0023]	1-7

☐ 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 document 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	Date of mailing of the international search report
24 April 2009	08/05/2009

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Horbach, Christian

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2008/068361

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
GB 2434950 A	08-08-2007	NONE	
WO 2006122433 A	23-11-2006	CA 2606574 A1	23-11-2006
		CN 101176299 A	07-05-2008
		EP 1886437 A1	13-02-2008
		JP 2008541633 T	20-11-2008
US 2006153364 A1	13-07-2006	NONE	

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2008/068361

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. H04L9/30

Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
H04L G07F

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.
X	GB 2 434 950 A (HEWLETT PACKARD DEVELOPMENT CO [US]) 8. August 2007 (2007-08-08) Seite 3, Zeilen 22-27 Seite 8, Zeile 3 - Seite 9, Zeile 5; Abbildung 2	1-7
A	WO 2006/122433 A (CERTICOM CORP [CA]; VANSTONE SCOTT A [CA]; BROWN DANIEL R L [CA]) 23. November 2006 (2006-11-23) Absätze [0014], [0015], [0022], [0023]	1-7
A	US 2006/153364 A1 (BEESON CURTIS L [US]) 13. Juli 2006 (2006-07-13) Absatz [0023]	1-7

☐ 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" älteres Dokument, 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 anderen 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	Absendedatum des internationalen Recherchenberichts
24. April 2009	08/05/2009

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Fax: (+31–70) 340–3016	Horbach, Christian

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2008/068361

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
GB 2434950 A	08-08-2007	KEINE	
WO 2006122433 A	23-11-2006	CA 2606574 A1	23-11-2006
		CN 101176299 A	07-05-2008
		EP 1886437 A1	13-02-2008
		JP 2008541633 T	20-11-2008
US 2006153364 A1	13-07-2006	KEINE	