Interner Verteilerschlüssel:

(A) [-] Veröffentlichung im ABl.
(B) [-] An Vorsitzende und Mitglieder
(C) [-] An Vorsitzende
(D) [X] Keine Verteilung

Datenblatt zur Entscheidung vom 15. Juni 2016

Beschwerde-Aktenzeichen: T 0939/13 - 3.5.05

Anmeldenummer: 07803214.1

Veröffentlichungsnummer: 2070250

IPC: H04L9/00, G06Q10/00

Verfahrenssprache: DE

Bezeichnung der Erfindung:
Verfahren zur Personalisierung von Dokumenten, kryptographisches System, Personalisierungssystem und Dokument

Anmelderin:
Bundesdruckerei GmbH

Stichwort:
Personalisierungssystem/BUNDESDRUCKEREI

Relevante Rechtsnormen:
EPÜ 1973 Art. 56

Schlagwort:
Erfinderische Tätigkeit - (ja, nach Änderungen)

Zitierte Entscheidungen:

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern
Boards of Appeal
Chambres de recours

European Patent Office
D-80298 MUNICH
GERMANY
Tel. +49 (0) 89 2399-0
Fax +49 (0) 89 2399-4465

Beschwerde-Aktenzeichen: T 0939/13 - 3.5.05

E N T S C H E I D U N G
der Technischen Beschwerdekammer 3.5.05
vom 15. Juni 2016

Beschwerdeführerin: (Anmelderin)
Bundesdruckerei GmbH
Oranienstrasse 91
10985 Berlin (DE)

Vertreter:
Richardt Patentanwälte PartG mbB
Wilhelmstraße 7
65185 Wiesbaden (DE)

Angefochtene Entscheidung:
Entscheidung der Prüfungsabteilung des Europäischen Patentamts, die am 18. Oktober 2012 zur Post gegeben wurde und mit der die europäische Patentanmeldung Nr. 07803214.1 aufgrund des Artikels 97 (2) EPÜ zurückgewiesen worden ist.

Zusammensetzung der Kammer:

Vorsitzende A. Ritzka
Mitglieder: K. Bengi-Akyuerek
G. Weiss

Sachverhalt und Anträge

I. Die Beschwerde richtet sich gegen die Entscheidung der Prüfungsabteilung auf Zurückweisung der vorliegenden europäischen Patentanmeldung aufgrund mangelnder erfinderischer Tätigkeit (Artikel 56 EPÜ) bezüglich eines Hauptantrags und zweier Hilfsanträge (Hilfsanträge I und II) gegenüber dem folgenden Stand der Technik:

D5: WO-A-01/59720.

Zudem wurde im Prüfungsverfahren und in der angefochtenen Entscheidung folgende Druckschrift zitiert:

D6: US-B-6 367 011.

II. Mit der Beschwerdebegründung reichte die Beschwerdeführerin einen neuen Anspruchssatz gemäß einem "modifizierten Hauptantrag" ein. Die Beschwerdeführerin beantragte, die angefochtene Entscheidung aufzuheben und ein Patent auf der Grundlage des Hauptantrags oder des modifizierten Hauptantrags oder hilfsweise auf der Basis eines der Hilfsanträge I und II zu erteilen.

III. Mit einem Bescheid nach Regel 100(2) EPÜ teilte die Kammer ihre vorläufige Meinung zur Beschwerde mit. Hierbei erhob sie insbesondere Einwände unter Artikel 56 EPÜ 1973, hauptsächlich gegenüber D5 und der von der Kammer als Beleg für das allgemeine Fachwissen des Fachmanns in das Beschwerdeverfahren eingeführten Druckschrift

D8: B. Martin: "Personalisierungssysteme für

Chipkarten", Diplomarbeit an der Universität Klagenfurt, Verlag Diplom.de, Seiten 75-139, 2002.

IV. Mit einem Antwortschreiben führte die Beschwerdeführerin Gegenargumente zu den Einwänden der Kammer an und gab zu verstehen, dass sie an ihren Anträgen festhielt.

V. Mit der Anlage zur Ladung für eine mündliche Verhandlung gemäß Artikel 15(1) VOBK erwiderte die Kammer die Gegenargumente der Beschwerdeführerin und bekräftigte ihre Einwände nach Artikel 56 EPÜ 1973.

VI. Mit Schreiben vom 12. Mai 2016 reichte die Beschwerdeführerin einen geänderten Anspruchssatz gemäß einem neuen Hilfsantrag II ein.

VII. Am 15. Juni 2016 fand die anberaumte mündliche Verhandlung statt, in deren Verlauf die Beschwerdeführerin einen neuen Hauptantrag als Reaktion auf die Einwände der Kammer nach Artikel 56 EPÜ 1973 einreichte. Der Schlussantrag der Beschwerdeführerin war, die Entscheidung über die Zurückweisung der europäischen Patentanmeldung aufzuheben und ein Patent zu erteilen auf der Grundlage des in der mündlichen Verhandlung eingereichten neuen Hauptantrags oder des mit der Beschwerdebegründung eingereichten modifizierten Hauptantrags oder des der angefochtenen Entscheidung zugrundeliegenden Hilfsantrags I oder des mit Schreiben vom 12. Mai 2016 eingereichten Hilfsantrags II. Am Ende der mündlichen Verhandlung wurde die Entscheidung der Kammer verkündet.

VIII. **Anspruch 1** des neuen Hauptantrags hat folgenden Wortlaut:

"Verfahren zur Personalisierung von Dokumenten (132), wobei jedes der Dokumente einen integrierten elektronischen Schaltkreis (130) aufweist, mit folgenden Schritten:

- Empfang von Eingangsdaten (110) für die Personalisierung der Dokumente durch ein Computersystem (102) einer Hochsicherheitsumgebung (100),
- Erzeugung eines Schlüsselpaars bestehend aus einem öffentlichen und einem privaten Schlüssel (142) für jedes der Dokumente, wobei die Erzeugung des Schlüsselpaars durch eine kryptographische Einheit (118) der Hochsicherheitsumgebung erfolgt,
- Instanziierung einer vorgegebenen Datenstruktur bestehend aus den Eingangsdaten und einem der öffentlichen Schlüssel für jedes der Dokumente durch das Computersystem,
- Erzeugung einer digitalen Signatur (152) der instanziierten Datenstruktur durch die kryptographische Einheit (118),
- Erzeugung von Steuerdaten (112) zur Personalisierung der Dokumente mit jeweils einer der instanziierten und signierten Datenstrukturen und dem der betreffenden instanziierten Datenstruktur zugeordneten privaten Schlüssel durch das Computersystem,
- Übertragung der Steuerdaten von dem Computersystem an eine Personalisierungsvorrichtung (114) einer Produktionsumgebung (101),
- Übertragung der instanziierten und signierten Datenstrukturen und der jeweils zugeordneten privaten Schlüssel von der Personalisierungsvorrichtung an die Dokumente gemäß den Steuerdaten,

- Speicherung der Datenstrukturen jeweils in einem Speicherbereich (138) des integrierten elektronischen Schaltkreises nach Prüfung der Signatur der Datenstrukturen, wobei die Speicherung unter einer Zugriffsbedingung erfolgt,
- Speicherung des privaten Schlüssels, der der jeweiligen Datenstruktur zugeordnet ist, in einem Speicherbereich (138) des integrierten elektronischen Schaltkreises, wobei die Speicherung so erfolgt, dass kein externer Zugriff auf den privaten Schlüssel möglich ist, wobei ein Ende-zu-Ende Verschlüsselungsverfahren zwischen der kryptographischen Einheit und den integrierten elektronischen Schaltkreisen der Dokumente verwendet wird, um die Übertragung der jeweiligen privaten Schlüssel zu schützen, wobei in der kryptographischen Einheit ein symmetrischer Schlüssel (154) gespeichert ist, und wobei der private Schlüssel mit Hilfe des symmetrischen Schlüssels durch die kryptographische Einheit verschlüsselt wird, so dass nur der verschlüsselte private Schlüssel an das Computersystem übertragen wird, und wobei in den integrierten Schaltkreisen derselbe symmetrische Schlüssel gespeichert ist, um den jeweiligen privaten Schlüssel vor dessen Speicherung zu entschlüsseln."

Der weitere unabhängige **Anspruch 5** des neuen Hauptantrags ist auf eine Vorrichtung gerichtet, deren strukturelle Merkmale den Verfahrensschritten von Anspruch 1 entsprechen.

Entscheidungsgründe

1. HAUPTANTRAG

Die unabhängigen Ansprüche 1 und 5 des neuen Hauptantrags unterscheiden sich insofern von den unabhängigen Ansprüchen des der angefochtenen Entscheidung zugrunde liegenden Hauptantrags, als sie zusätzlich angeben, dass

A) eine vorgegebene Datenstruktur bestehend aus den Eingangsdaten und einem öffentlichen Schlüssel instanziiert wird;
B) eine digitale Signatur der instanziierten Datenstruktur durch die kryptographische Einheit erzeugt wird;
C) instanziierte und signierte Datenstrukturen erzeugt und übertragen werden;
D) nach Prüfung der Signatur der Datenstrukturen die jeweiligen Datenstrukturen im integrierten elektronischen Schaltkreis gespeichert werden.

Die Änderung A) basiert z.B. auf der Offenbarung von Seite 7, Zeilen 3-4 oder Seite 12, Zeilen 8-10 der ursprünglich eingereichten Anmeldung. Änderung B) findet ihre Stütze in der Offenbarung von Seite 15, letzter Absatz in Verbindung mit Figur 2, Schritt 216, während die Änderung C) z.B. durch Seite 16, erster Absatz der ursprünglichen Anmeldung gestützt wird. Änderung D) basiert vornehmlich auf Seite 18, zweiter Absatz. Die obigen Änderungen erfüllen somit die Erfordernisse des Artikels 123(2) EPÜ.

1.1 Artikel 52(1) EPÜ: Neuheit und erfinderische Tätigkeit

Nach Beurteilung der Kammer erfüllen die unabhängigen

Ansprüche 1 und 5 des neuen Hauptantrags die Erfordernisse des Artikels 52(1) EPÜ in Verbindung mit Artikel 56 EPÜ 1973. Die Gründe hierfür sind wie folgt:

1.1.1 Anspruch 1 des Hauptantrags umfasst folgende einschränkenden Merkmale (gemäß der Merkmalsgliederung der Kammer):

Verfahren zur Personalisierung von Dokumenten, wobei jedes der Dokumente einen integrierten elektronischen Schaltkreis aufweist, mit folgenden Schritten:

a) Empfang von Eingangsdaten für die Personalisierung der Dokumente durch ein Computersystem einer Hochsicherheitsumgebung;

b) Erzeugung eines Schlüsselpaars bestehend aus einem öffentlichen und einem privaten Schlüssel für jedes der Dokumente, wobei die Erzeugung des Schlüsselpaars durch eine kryptographische Einheit der Hochsicherheitsumgebung erfolgt;

c) Instanziierung einer vorgegebenen Datenstruktur bestehend aus den Eingangsdaten und einem der öffentlichen Schlüssel für jedes der Dokumente durch das Computersystem;

d) Erzeugung einer digitalen Signatur der instanziierten Datenstruktur durch die kryptographische Einheit;

e) Erzeugung von Steuerdaten zur Personalisierung der Dokumente mit jeweils einer der instanziierten und signierten Datenstrukturen und dem der betreffenden instanziierten Datenstruktur zugeordneten privaten Schlüssel durch das Computersystem;

f) Übertragung der Steuerdaten von dem Computersystem an eine Personalisierungsvorrichtung einer Produktionsumgebung;

g) Übertragung der instanziierten und signierten Datenstrukturen und der jeweils zugeordneten privaten Schlüssel von der Personalisierungsvorrichtung an die Dokumente gemäß den Steuerdaten;

h) Speicherung der Datenstrukturen jeweils in einem Speicherbereich des integrierten elektronischen Schaltkreises nach Prüfung der Signatur der Datenstrukturen, wobei die Speicherung unter einer Zugriffsbedingung erfolgt;

i) Speicherung des privaten Schlüssels, der der jeweiligen Datenstruktur zugeordnet ist, in einem Speicherbereich des integrierten elektronischen Schaltkreises, wobei die Speicherung so erfolgt, dass kein externer Zugriff auf den privaten Schlüssel möglich ist;

wobei

j) ein Ende-zu-Ende Verschlüsselungsverfahren zwischen der kryptographischen Einheit und den integrierten elektronischen Schaltkreisen der Dokumente verwendet wird, um die Übertragung der jeweiligen privaten Schlüssel zu schützen;

k) in der kryptographischen Einheit ein symmetrischer Schlüssel gespeichert ist;

l) der private Schlüssel mit Hilfe des symmetrischen Schlüssels durch die kryptographische Einheit verschlüsselt wird, so dass nur der verschlüsselte private Schlüssel an das Computersystem übertragen wird;

m) in den integrierten Schaltkreisen derselbe symmetrische Schlüssel gespeichert ist, um den jeweiligen privaten Schlüssel vor dessen Speicherung zu entschlüsseln.

1.1.2 Die Kammer teilt die Auffassung der Prüfungsabteilung, dass die Druckschrift **D5** durchaus als ein geeigneter

Ausgangspunkt für die Bewertung der erfinderischen Tätigkeit des vorliegenden Gegenstandes angesehen werden kann, da sie sich mit der Personalisierung von chipkarten-basierten elektronischen Dokumenten mittels kryptographischen Schlüsseln befasst. Auch wenn die auf Figur 2C von D5 basierende Ausführungsform nicht die eigentliche "Erfindungsidee" von D5, wie von der Beschwerdeführerin mehrmals vorgebracht, darstellen sollte, belegt sie doch zutreffend, dass die erfindungsgemäße Personalisierungsinfrastruktur in der Tat zum Prioritätszeitpunkt der Anmeldung bekannt war.

Die Ausführungsform gemäß Figur 2C von D5 sieht nämlich - wie die vorliegende Erfindung - eine Trennung zwischen der Personalisierungsdatenaufbereitung an einer Stelle und dem eigentlichen Personalisierungs-prozess an einer anderen Stelle vor (vgl. Seite 7, Zeile 18 bis Seite 10, Zeile 8), auch wenn sie mit gewissen Nachteilen verbunden sein sollte (siehe z.B. Seite 8, Zeilen 32-35). Diese bekannten Nachteile betreffen jedoch lediglich den resultierenden Zeitaufwand und die Implementierungskosten, nicht aber die entsprechenden Sicherheitsanforderungen an das System. Indes wird in D5 über die Vor- und Nachteile hinsichtlich der Sicherheitsaspekte im Vergleich zwischen den Ausführungsformen von Figur 2C und Figur 3 in technischer Hinsicht nichts Einschränkendes ausgesagt.

1.1.3 Hinsichtlich **Merkmal a)** offenbart D5 im Zusammenhang mit der Ausführungsform eines Personalisierungssystems gemäß Figur 2C, dass ein Computersystem ("P3 processing system 120") Personalisierungsdaten ("cardholder data") empfängt (siehe z.B. Seite 7, Zeilen 22-32 und Fig. 2A, Schritt 210). Dieses Computersystem befindet sich zudem - im Gegensatz zur in der Beschwerdebegründung

hervorgehobenen Ausführungsform gemäß Figur 3 von D5 - *innerhalb* des Kartenausgabesystems (siehe Seite 7, Zeilen 25-26). Da wiederum ein Kartenausgabesystem, das stets sensitive Personalisierungsdaten zu verwalten hat, typischerweise hohen Sicherheitsanforderungen genügen muss, kann die "in-house"-Umgebung gemäß der Terminologie von D5 durchaus mit einer "Hochsicherheitsumgebung" im Sinne von Merkmal a) gleichgesetzt werden. Hierbei schließt sich die Kammer der Einschätzung der Prüfungsabteilung an, dass selbst wenn eine solche (wie auch immer definierte) "Hochsicherheitsumgebung" als ein sogenanntes "Trust-Center" nach der Lehre der ursprünglichen Anmeldung ausgebildet sein sollte (siehe z.B. Seite 9, Zeilen 1-2), dies den Anspruch technisch nicht entscheidend einschränken würde (vgl. angefochtene Entscheidung, Gründe 3.2.2).

In Bezug auf **Merkmal b)** lehrt D5, dass die zu verwendenden Chipkarten nicht nur symmetrische, sondern auch *asymmetrische* Kryptoverfahren unterstützen können müssen (siehe z.B. Seite 15, Zeilen 17-19), was inhärenterweise mit der Erzeugung eines aus einem öffentlichen wie privaten Schlüssel bestehenden Schlüsselpaars für die zu personalisierenden Chipkarten einhergeht. Obwohl in D5 zudem erwähnt wird, dass die kryptographischen Schlüssel in einer Einheit ("Hardware Security Module HSM 124") der "in-house"-Umgebung in sicherer Weise gespeichert werden (siehe z.B. Seite 8, Zeilen 23-31), wird jedoch nicht genau beschrieben, in welcher Einheit die jeweiligen Schlüsselpaare tatsächlich *generiert* werden.

Hinsichtlich **Merkmal c)** offenbart D5 überdies, dass das Computersystem eine vorgegebene Datenstruktur ("personalization file of cardholder") mit den

Eingangsdaten erstellt, d.h. instanziiert (siehe z.B. Seite 7, Zeilen 25-32 in Verbindung mit Fig. 2A, Schritt 230). Hierbei wird jedoch nicht explizit angegeben, ob der entsprechende öffentliche Schlüssel bei einer solchen Instanziierung in die Datenstruktur eingetragen wird.

Bezüglich **Merkmale e)** und **f)** lehrt D5, dass das Computersystem Steuerdaten ("personalization file") zur Personalisierung der Chipkarten erzeugt und an eine Personalisierungsvorrichtung ("card personalisation system 130") überträgt (siehe Fig. 2B, Schritt 240). In diesem Zusammenhang wird auch die Möglichkeit erwähnt, dass diese Personalisierungsvorrichtung *außerhalb* der "in-house" Umgebung, nämlich an einer externen Personalisierungsstelle, angeordnet ist (siehe Seite 7, Zeilen 32-34). Diese externe Personalisierungsstelle kann somit durchaus auf eine "Produktionsumgebung" gemäß Merkmal f) gelesen werden. Indes wird die Übertragung des privaten Schlüssels zusammen mit den Steuerdaten hier nicht eindeutig offenbart.

Hinsichtlich **Merkmal g)** beschreibt D5, dass die Steuerdaten von der Personalisierungsvorrichtung ihrerseits an die Chipkarten übertragen und dort gespeichert werden (siehe z.B. Seite 7, Zeilen 10-15 und Fig. 2B, Schritt 250). In diesem Zusammenhang würde der fachkundige Leser auch mitlesen, dass die generierten, für die Personalisierung nötigen kryptographischen Schlüssel ("cryptographic keys") auch an die zu personalisierenden Chipkarten *übertragen* und dort *gespeichert* werden müssen. Von einer digitalen Signierung der betreffenden Daten auf der Sendeseite und deren Überprüfung auf der Empfangsseite ist jedoch keine Rede.

Bezüglich der Speicherung der übertragenen Daten gemäß **Merkmale h)** und **i)** versteht es sich nach Auffassung der Kammer von selbst, dass diese zu speichernden sensitiven Daten in D5 notwendigerweise gegenüber externen Zugriffen geschützt werden und daher hier - zumindest implizit - auch Zugriffsbedingungen vorliegen müssen.

In Bezug auf die **Merkmale j)** bis **m)**, welche die Sicherung des zu übertragenden privaten Schlüssels betreffen, erwähnt D5 die Speicherung von kryptographischen Schlüsseln zur Bereitstellung einer "transport security" und die Verwendung eines "Key Encrypting Key (KEK)" (siehe Seite 5, Zeilen 15-20). Hierunter versteht die Kammer, dass eine sichere Kommunikation auf der Transportschicht des OSI-Modells (Ende-zu-Ende-Übertragungsschicht) in der Initialisierungsphase ermöglicht werden soll. Es wird aber nicht weiter erläutert, um welche konkreten Schlüsseltypen (z.B. asymmetrische bzw. symmetrische Schlüssel) es sich hierbei handelt.

1.1.4 Der Gegenstand von Anspruch 1 unterscheidet sich somit von der Offenbarung von D5 darin, dass

1) die kryptographische Einheit
   i) eine digitale Signatur der aus Eingangsdaten und einem öffentlichen Schlüssel bestehenden instanziierten Datenstruktur erzeugt;
   ii) das asymmetrische Schlüsselpaar erzeugt und den privaten Schlüssel mit einem in der Einheit gespeicherten symmetrischen Schlüssel verschlüsselt.
2) das Computersystem

i) die instanziierten und signierten Datenstrukturen als Steuerdaten an die Personalisierungsvorrichtung überträgt;

ii) den zugeordneten verschlüsselten privaten Schlüssel zusammen mit den Steuerdaten an die Personalisierungsvorrichtung überträgt;

3) die Personalisierungsvorrichtung

i) die instanziierten und signierten Datenstrukturen an die Dokumente überträgt;

ii) den verschlüsselten privaten Schlüssel an die Dokumente überträgt;

4) die Dokumente

i) die übertragenen Datenstrukturen nach Prüfung der Signatur der Datenstrukturen in einem Speicherbereich des integrierten elektronischen Schaltkreises speichern;

ii) zur Entschlüsselung des jeweiligen verschlüsselten privaten Schlüssels den von der kryptographischen Einheit verwendeten symmetrischen Schlüssel im integrierten elektronischen Schaltkreis speichern.

1.1.5 Offensichtlich betreffen die Unterscheidungsmerkmale 1i), 2i), 3i) und 4i) die kryptographische Sicherung der an die jeweilige Chipkarte zu übertragenden *Personalisierungsdaten (Eingangsdaten)* und des *öffentlichen Schlüssels*, während die Unterscheidungsmerkmale 1ii), 2ii), 3ii) und 4ii) der Sicherung des *privaten Schlüssels* zuzuordnen sind. Die synergetische technische Wirkung dieser Unterscheidungsmerkmale besteht nach Einschätzung der Kammer in der *gemeinsamen* Übertragung von *getrennt* gesicherten Personalisierungsinformationen, d.h. den eigentlichen Personalisierungsdaten zusammen mit dem öffentlichen Schlüssel auf der einen Seite (gesichert durch eine digitale Signatur) und den privaten

Schlüssel auf der anderen Seite (gesichert durch eine eigene Verschlüsselung).

Die Kammer sieht mithin die durch Anspruch 1 zu lösende objektive technische Aufgabe darin, "die Abhör- und Fälschungssicherheit der an die Chipkarten übertragenen Personalisierungsinformationen zu erhöhen ohne hierbei die Übertragungseffizienz zu beeinträchtigen".

1.1.6 Was zunächst die isolierte Betrachtung der Unterscheidungsmerkmale 1ii), 2ii), 3ii) und 4ii) angeht, teilt die Kammer prinzipiell die Auffassung der Prüfungsabteilung, dass diese - für sich alleine betrachtet - nicht auf einer erfinderischen Tätigkeit beruhen (vgl. angefochtene Entscheidung, Gründe 3.2). Der Fachmann auf dem Gebiet der Chipkartenkryptographie wüsste nämlich, dass insbesondere der geheime, private Schlüssel einer Chipkarte besonders vor potenziellen Abhörangriffen zu schützen ist und würde nach Auffassung der Kammer den Hinweis in D5 sofort aufgreifen, dass auch ein Verschlüsselungsschlüssel durch einen anderen Schlüssel ("Key Encryption Key KEK") verschlüsselt werden kann (siehe Seite 15, Zeilen 25-30). Zudem ist davon auszugehen, dass zum Prioritätszeitpunkt der Anmeldung auch die Verschlüsselung von privaten Schlüsseln durch symmetrische (oder auch asymmetrische) Schlüssel nach dem sogenannten "Envelope-Prinzip" zur Erhöhung der Abhörsicherheit von privaten Schlüsseln dem Fachmann der Kryptographie hinreichend bekannt war (siehe z.B. **D8**, Seite 86, erster Absatz oder **D6**, Spalte 8, Zeilen 17-34 in Verbindung mit Fig. 4).

1.1.7 Die übrigen Unterscheidungsmerkmale 1i), 2i), 3i) und 4i), die sich auf das separat erfolgende digitale Signieren sowohl der eigentlichen

Personalisierungsdaten als auch des in der instanziierten Datenstruktur enthaltenen öffentlichen Schlüssels beziehen, sind jedoch für sich genommen nicht aus dem vorliegenden Stand der Technik bekannt oder nahegelegt, geschweige denn in Kombination und in Wechselwirkung mit den Merkmalen 1ii), 2ii), 3ii) und 4ii). Zudem kann diese zusätzliche kryptographische Maßnahme nach Auffassung der Kammer auch nicht als rein administrative und damit nicht-technische Vorgabe betrachtet werden, wie an mehreren Stellen der angefochtenen Entscheidung im Zusammenhang mit anderen Merkmalen von Anspruch 1 angeführt wurde (vgl. angefochtene Entscheidung, Gründe 3.2.3 bis 3.2.6).

Im Zusammenhang mit den Merkmalen 1i), 2i), 3i) und 4i) erschöpft sich nämlich **D5** in der bloßen Erwähnung einer eventuell möglichen Integritätssicherung von nicht näher benannten Daten (z.B. mittels gewöhnlicher "Message Authentication Codes (MAC)" gemäß Seite 15, Zeilen 30-34 bzw. mittels zweier Signaturen zur Aktualisierung eines Kreditkartenparameters nach Seite 21, Zeilen 28-29 oder mit Hilfe der Signierung eines Sicherheitssoftwaremoduls gemäß Seite 23, Zeilen 2-6). Darüber hinaus sind dieser Druckschrift jedoch keinerlei Hinweise oder Anreize zur Implementierung von zusätzlichen kryptographischen Maßnahmen wie der getrennten Signierung der Personalisierungsdaten und des entsprechenden öffentlichen Schlüssels, unabhängig von der Sicherung des zugehörigen privaten Schlüssels, zu entnehmen - ganz abgesehen von deren gemeinsamen Übertragung in einem Übertragungsvorgang, d.h. mit einer Nachricht.

Indes beschreibt die Diplomarbeit **D8** zwar die Übertragung eines "chipkartenindividuellen Personalisierungsschlüssels *cKP*" (d.h. eines privaten

Schlüssels) von einem Sicherheitsmodul an die zu personalisierende Chipkarte in einer *Initialisierungsphase* (siehe Seite 126, Abb. 4.13) und die Übertragung von durch diesen privaten Schlüssel *cKP* verschlüsselten Personalisierungsdaten DS mit Hilfe einer Personalisierungsmaschine an die Chipkarte in einer *Personalisierungsphase*. Im Hinblick auf die obigen Unterscheidungsmerkmale ist jedoch festzustellen, dass hier weder die getrennte Sicherung von Personalisierungsdaten mitsamt öffentlichem Schlüssel bzw. privatem Schlüssel noch die simultane Übertragung dieser Informationen eine Rolle spielen. Ausgehend von der objektiven technischen Aufgabe würde der Fachmann bestenfalls veranlassen, dass der private Schlüssel nach dem "Envelope"-Prinzip verschlüsselt wird und/oder dass die Initialisierungs- und Personalisierunsphasen aus Effizienzgründen zusammengelegt werden.

Das Dokument **D6** wiederum offenbart die Erzeugung und Verwendung von asymmetrischen Schlüsselpaaren (siehe z.B. Spalte 11, Zeilen 19-35 und Fig. 1), enthält jedoch keinerlei Anreize, einerseits die Personalisierungsdaten mitsamt öffentlichem Schlüssel zu signieren und andererseits den privaten Schlüssel zu verschlüsseln, um die gesicherten Daten in *einem* Übertragungsvorgang gemeinsam von einem Computersystem ("preparation processing device 154") über eine Personalisierungsvorrichtung ("personalization device 150") an die jeweilige Chipkarte zu übertragen.

Folglich würde der Fachmann, ausgehend von D5, D8 oder auch D6, nicht in naheliegender Weise zur Lösung gemäß Anspruch 1 gelangen.

1.2 Die Kammer folgert aus den obigen Feststellungen, dass der Gegenstand von Anspruch 1 des neuen Hauptantrags, im Lichte des in der angefochtenen Entscheidung berücksichtigten Standes der Technik, neu ist und auf einer erfinderischen Tätigkeit beruht (Artikel 52(1) EPÜ in Verbindung mit Artikel 54 and 56 EPÜ 1973). Da zudem die strukturellen Merkmale des unabhängigen Vorrichtungsanspruchs 5 den Merkmalen von Anspruch 1 entsprechen (siehe Punkt VIII oben), gilt diese Schlussfolgerung auch für Anspruch 5 des neuen Hauptantrags.

2. Aufgrund der Ansicht der Kammer, dass auch alle anderen Erfordernisse des EPÜ erfüllt sind, steht einer Patenterteilung gemäß dem neuen Hauptantrag nichts mehr im Wege. Die vorliegenden nachrangigen Hilfsanträge müssen folglich auch nicht weiter betrachtet werden.

Entscheidungsformel

Aus diesen Gründen wird entschieden:

1. Die angefochtene Entscheidung wird aufgehoben.

2. Die Angelegenheit wird an die erste Instanz mit der Anordnung zurückverwiesen, ein Patent mit folgender Fassung zu erteilen:

   Beschreibung (Seiten):
   - 1-3, 6-12, 14-22 der veröffentlichten Fassung;
   - 4, 4a eingereicht am 1. Dezember 2010 mit Telefax;
   - 5, 5a, 13 eingereicht am 6. Juli 2012 in elektronischer Form.

   Ansprüche (Nr.):
   1 bis 10 gemäß Hauptantrag eingereicht in der mündlichen Verhandlung vor der Beschwerdekammer.

   Zeichnungen (Blätter):
   1/4-4/4 der veröffentlichten Fassung.

Die Geschäftsstellenbeamtin: Die Vorsitzende:

L. Malécot-Grob A. Ritzka

Entscheidung elektronisch als authentisch bestätigt