

# Sicherheitsanwendungen auf Basis intelligenter Speicherpolymere

T. Hupe<sup>1</sup> · S. Völkening<sup>2</sup> · H. Jüngermann<sup>3</sup>

Bayer Innovation GmbH

<sup>1</sup> [torsten.hupe@bayer-innovation.de](mailto:torsten.hupe@bayer-innovation.de)

<sup>2</sup> [stephan.voelkening@bayer-innovation.de](mailto:stephan.voelkening@bayer-innovation.de)

<sup>3</sup> [hardy.juengermann@bayer-innovation.de](mailto:hardy.juengermann@bayer-innovation.de)

## Zusammenfassung

Gegenstand des Vortrags ist ein System zur automatisierten Authentifizierung von Personen. Die Authentifizierung geschieht durch Verifikation, d.h. durch den Abgleich biometrischer Merkmale mit entsprechenden Referenzdaten, die auf einer ID-Karte abgelegt sind.

Die Besonderheit des Systems liegt in den ID-Karten, auf denen die Referenzdaten unsichtbar und *hardware*verschlüsselt gespeichert sind. Möglich gemacht wird dies durch ein Speichermedium aus so genannten photoadressierbaren Polymeren. In diese intelligenten Speicherpolymere lassen sich Informationen mit Licht einschreiben und auslesen. Eine spezielle holographische Verschlüsselungsmethode schützt vor ungewolltem Auslesen und vor Manipulation.

Aufgrund der hohen Fälschungssicherheit ist das Authentifizierungssystem für Hochsicherheits-Bereiche prädestiniert.

Die hohe Speicherkapazität, über die das polymere Speichermedium verfügt, eröffnet aber noch weitere Einsatzgebiete, wie z.B. die Verwendung in einer Gesundheitskarte.

## 1 Einleitung

Durch die wachsende Vernetzung und die zunehmende Globalisierung der Gesellschaft wird es immer wichtiger, dass jede einzelne Person in die Lage versetzt wird, sich eindeutig zu authentifizieren.

Früher reichte im Allgemeinen ein Personalausweis, um eine Identität nachweisen zu können. In Folge der zunehmenden maschinellen Datenverarbeitung verfügt ein Mensch heute

zusätzlich über einen Firmenausweis, einen Krankenkassenausweis, eine Kredit- oder EC-Karte – alles Instrumente, mit denen er nachweisen kann, dass er derjenige ist, den er vorgibt zu sein. Diese Grundlage verschafft ihm Zugang zu seinem Arbeitsplatz, zu Krankenkassenleistungen, zu seinem Konto usw.

Und ein Ende der Einsatzmöglichkeiten ist noch nicht abzusehen. Bereits intensiv diskutiert wird die Einführung der Gesundheitskarte [Bund04], daneben gibt es Überlegungen zu einer Jobkarte und anderen Ausweissystemen [Schulz04].

Allen Ausweissystemen ist gemeinsam, dass zwischen Ausweis und Besitzer eine eindeutige Zuordnung bestehen muss. Diese Zuordnung wird durch charakteristische Merkmale des Besitzers hergestellt, die in den Ausweis aufgenommen werden (z.B. Passfoto, Personalnummer, Fingerabdruck o.ä.). Anhand dieser Merkmale kann die Identität einer Person festgestellt (Identifikation) oder überprüft (Verifikation) werden.

Ferner muss eine hinreichende Fälschungssicherheit gegeben sein. Es muss verhindert werden, dass sich eine Person als eine andere ausgibt.

Je nach Anwendung werden noch weitere spezielle Anforderungen an die jeweiligen Ausweissysteme gestellt. Aus der Sicht des Benutzers ist zum Beispiel die Wahrung der Privatsphäre essentiell. Gerade wenn, wie im Fall der Gesundheitskarte, vertrauliche Daten auf dem Ausweis gespeichert sind, muss gewährleistet sein, dass ein Auslesen der Karte nur mit der Einwilligung des Besitzers geschieht. Ein Auslesen durch nicht autorisierte Personen muss verhindert werden.

Im Rahmen der zunehmenden Automatisierung ist die Maschinenlesbarkeit eine weitere Forderung.

## **2 Ein Ausweissystem für Hochsicherheitsanforderungen**

Im Folgenden soll ein Ausweissystem vorgestellt werden, das den genannten Anforderungen gerecht wird. Die eindeutige Zuordnung zwischen Ausweis und Besitzer wird über biometrische Merkmale hergestellt. Die Merkmale werden in Form von Referenzdaten holographisch verschlüsselt in ein Speichermedium aus so genanntem photadressierbarem Polymer abgelegt. Diese Speichertechnik erlaubt hohen Schutz gegenüber Fälschung, Manipulation aber auch ungewolltem Auslesen. Eine Authentifizierung geschieht willentlich durch den Besitzer, indem er seine Karte in ein Lesegerät steckt. Es folgt der Abgleich eines seiner biometrischen Merkmale mit den Referenzdaten auf der Karte. Bei Übereinstimmung hat er sich authentifiziert.

Die Elemente des Systems sowie ihre Schutzmechanismen werden im Folgenden näher vorgestellt.

### **2.1 Biometrie: Eindeutige Zuordnung von Ausweis und Besitzer**

Im derzeitigen deutschen Personalausweis sind die bibliographischen Daten einer Person und ein Lichtbild abgelegt [Bund05]. Diese Informationen dienen zum einen der Identifikation der Person (*Wer ist die Person?*), zum anderen der Verifikation (*Passen die Merkmale wie Alter, Größe und Lichtbild zu der Person?*). Schließlich ist eine Reihe von Elementen integriert,

welche die Echtheit des Dokuments garantieren sollen (Integrität). Alle Informationen sind so ausgelegt, dass sie durch einen menschlichen Betrachter geprüft werden können.

Für eine automatisierte, maschinelle Authentifizierung werden maschinenlesbare Ausweise benötigt. Ferner ist eine automatisierte Erkennung von Personen erforderlich. Hierfür werden charakteristische Merkmale einer Person herangezogen, so genannte biometrische Merkmale, die eine eindeutige Zuordnung zu einer Person gewährleisten sollen, z.B. Fingerabdruck, Irismuster, Handgeometrie, Gesichtsbild oder Stimme [Wiki05].

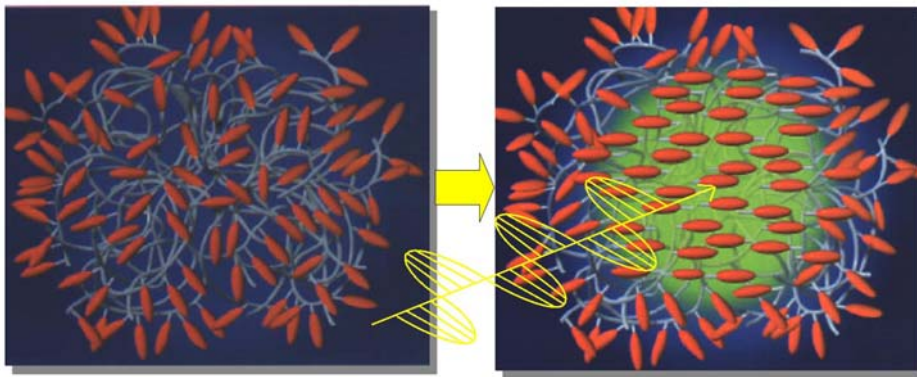
Die biometrischen Merkmale können in Form von Referenzdaten zentral in einer Datenbank gespeichert oder (dezentral) auf dem Ausweis abgelegt werden. Aus datenschutzrechtlichen Gründen ist eine dezentrale Speicherung stets vorzuziehen, so dass der Ausweis über ein geeignetes Speichermedium verfügen muss. Die Anforderungen an das Speichermedium sind:

- **Ausreichende Speicherkapazität:** biometrische Merkmale benötigen mehr Speicher als bibliographische Daten. Legt man die Empfehlungen der ICAO für maschinenlesbare Reisepässe zu Grunde, ergibt sich folgender Speicherbedarf [ICAO04]: 12 K für Bilder zur Gesichtserkennung, 10 K für Bilder von Fingerabdrücken, 30 K für Bilder zur Iriserkennung.  
Bei der Verwendung multipler biometrischer Merkmale und mehrerer Referenzdatensätze zur Steigerung der Zuverlässigkeit bei der Erkennung erreicht die erforderliche Speicherkapazität schnell 100 K.
- **Schutz vor ungewolltem Auslesen:** Zur Gewährleistung der Privatsphäre einer Person sollen die biometrischen Merkmale verschlüsselt abgelegt werden. Neben dieser digitalen Datenverschlüsselung ist ein Hardware-Schutz vor ungewolltem Auslesen wünschenswert.
- **Fälschungssicherheit:** Diese Forderung bezieht sich auf das gesamte Ausweisdokument. Die Sicherheitselemente müssen maschinell überprüfbar sein. Um die Komplexität eines Lesegeräts für das Ausweisdokument in Grenzen zu halten, bietet es sich an, Teile der Echtheitsprüfung auf das Speichermedium zu verlagern, da dieses ohnehin maschinell lesbar gestaltet ist.

Diese Anforderungen werden durch das im Folgenden näher beschriebene Speichermedium erfüllt.

## 2.2 Intelligente Polymere

Das Speichermaterial besteht aus einem so genannten photoadressierbaren Polymer. Es ist licht-aktiv, d.h. bestimmte Molekülgruppen im Polymer reagieren auf Lichteinstrahlung, indem sie sich ausrichten, wenn polarisiertes Licht einer bestimmten Wellenlänge auf sie trifft [HaBi01]. Dieser Vorgang ist in Abb. 1 illustriert.



**Abb. 1:** Durch Bestrahlen mit polarisiertem Laserlicht richten sich die Polymermoleküle im Speichermedium aus. Die Ausrichtung bleibt auch bei Abschalten des Lichts erhalten, so dass sich auf diese Weise Informationen einschreiben lassen.

Informationen ließen sich in dem Speichermedium wie auf einer CD oder DVD abspeichern, d.h. digital in Form von Nullen und Einsen, wobei Domänen mit senkrecht orientierten Polymermolekülen z.B. Einsen darstellen, Domänen mit waagrecht orientierten Polymermolekülen Nullen. Eine solche Speicherung hat jedoch den Nachteil, dass sie durch Unberechtigte ausgelesen werden kann; es bedarf lediglich eines polarisierten Lichtstrahls.

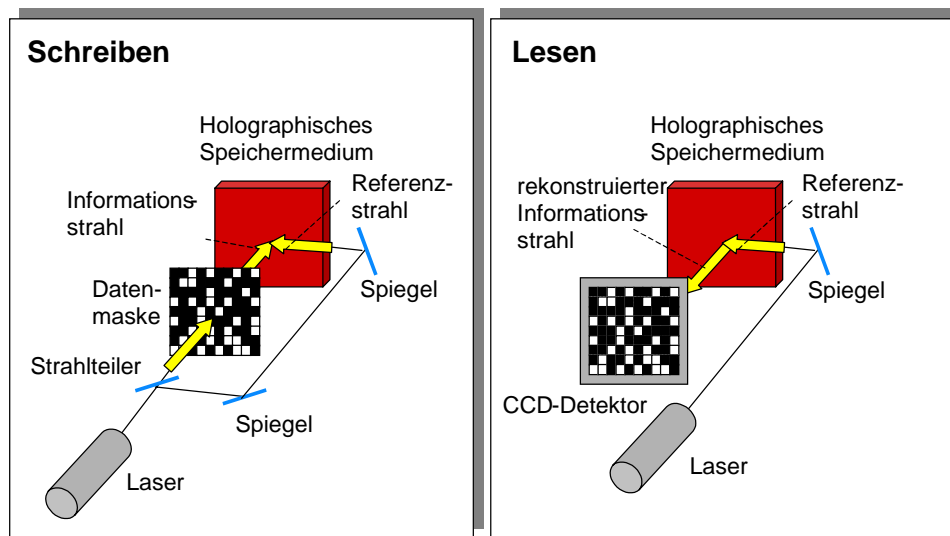
### 2.3 Holographische Datenspeicherung

Beim vorliegenden Speichersystem werden die Informationen holographisch gespeichert. Ein Hologramm ist ein Interferenzmuster, das durch Überlagerung von zwei Laserstrahlen entsteht [Hari02]. Dies ist in Abb. 2 illustriert.

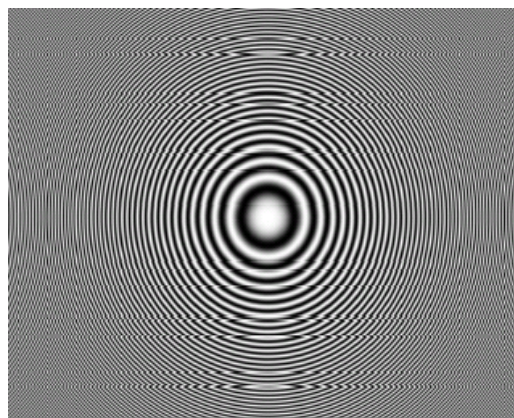
Während bei optisch digital gespeicherten Informationen eine Reihe von Nullen und Einsen direkt einer Informationseinheit zugeordnet werden kann, ist eine Informationseinheit im Hologramm über die gesamte Fläche „verschmiert“. Zerbricht man das Hologramm in zwei Teile, so erhält man bei Bestrahlen der einzelnen Teile jeweils zwei komplette Bilder, die etwas kontrastärmer sind als das ursprüngliche Bild. Daraus folgt, dass die Manipulation z.B. eines Teils der Daten ausgeschlossen ist.

Die Holographie stellt eine Art der Hardware-Verschlüsselung dar. Die gespeicherte Information kann nur durch Bestrahlung mit dem Referenzstrahl, der beim Einschreiben verwendet wurde, sichtbar gemacht werden. Der Referenzstrahl lässt sich kodieren, d.h. er kann in spezieller Weise moduliert werden. Nur wer die Modulation kennt, kann die Daten lesen (siehe nächsten Abschnitt).

Die Speicherdichte des Verfahrens ist sehr hoch; auf einer Speicherkarte in der Größe einer Kreditkarte lassen sich mehrere Hundert MByte unterbringen.



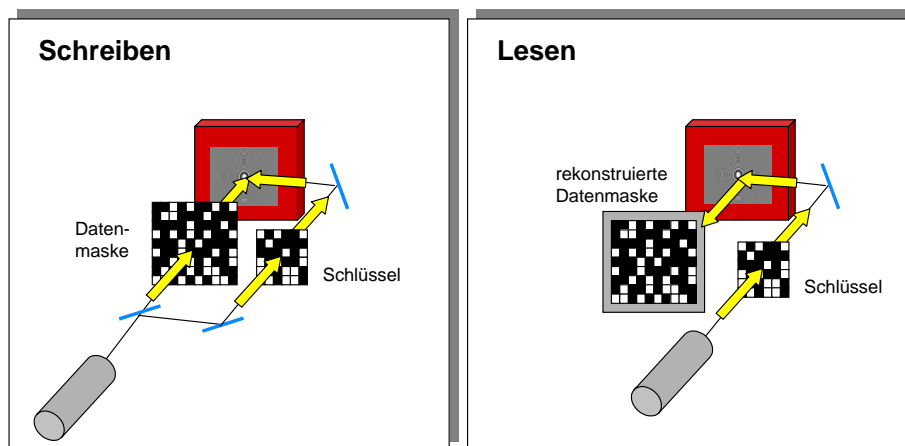
**Abb. 2:** Schematische Darstellung eines holographischen Speicherverfahrens. Die Informationen werden in Form von Datenmasken eingeschrieben. Dabei wird nicht die Datenseite selbst gespeichert, sondern die holographisch verschlüsselte Datenseite: Ein Laserstrahl wird zunächst in zwei Teilstrahlen aufgeteilt. Der eine Teilstrahl wird durch eine Maske geleitet. Auf diese Weise werden dem Strahl die zu speichernden Informationen aufgeprägt. Der zweite Teilstrahl ist der so genannte Referenzstrahl. Dieser wird so umgeleitet, dass er mit dem Informationsstrahl im photoadressierbaren Polymer überlagert wird. Dadurch entsteht in dem Speichermedium ein spezielles Muster, das Hologramm. Durch Bestrahlen dieses Hologramms mit dem Referenzstrahl lässt sich der Informationsstrahl reproduzieren und die gespeicherte Information auf einem Detektor sichtbar machen.



**Abb. 3:** Hologramm. Die Information ist nicht lokalisierbar, sondern als Interferenzmuster über das gesamte Hologramm „verschmiert“.

## 2.4 Verschlüsselung

Die Kodierung des Referenzstrahls erfolgt auf Hardware-Ebene mit einer Maske (siehe Abb. 4). Sollen Daten für verschiedene Anwendungen auf die Karte gespeichert werden, werden verschiedene Masken verwendet: Die Bank erhält ein Lesegeräte mit der Maske A, mit der die Bankdaten auf der Karte verschlüsselt sind, der Arzt ein Lesegeräte mit der Maske B, mit der die medizinischen Informationen verschlüsselt sind. Die Masken A und B sind nicht miteinander kompatibel, d.h. Informationen lassen sich nicht unter Verwendung einer anderen Maske aus dem Speichermaterial auslesen.



**Abb. 4:** Schematische Darstellung der Hardware-Verschlüsselung bei der holographischen Datenspeicherung. Nur wenn der Referenzstrahl mit der richtigen Schlüsselmaske moduliert wird, kann die vorher eingeschriebene Datenmaske rekonstruiert werden.

## 2.5 Authentifizierungssystem für Hochsicherheitsanwendungen

Ein Authentifizierungssystem für Hochsicherheitsanwendungen lässt sich anhand der vorgestellten Komponenten wie folgt realisieren: Berechtigte Personen erhalten eine ID-Karte, auf der neben bibliographischen Informationen wie dem Namen biometrische Merkmale holographisch verschlüsselt gespeichert sind. Zugangskontrollpunkte sind mit einem Kartenlesegerät und einem Sensor für die Aufnahme eines biometrischen Merkmals ausgestattet. An diesen Kontrollpunkten signalisiert der Besitzer einer Karte bewusst den Wunsch nach Zugang durch Einführen der Karte in das Lesegerät.

Als erstes wird anhand des Namens oder einer Referenznummer überprüft, ob die Person registriert ist. Dann wird über den Sensor ein biometrisches Merkmal erfasst (z.B. Fingerabdruck oder Irismuster) und mit den Referenzdaten auf der Karte verglichen. Stimmen die Daten überein, erhält die Person Zugang. Stimmen sie nicht überein, wird die Person abgewiesen. Dasselbe geschieht, wenn die Karte unlesbar oder die Person nicht registriert ist.

Ein sicheres Ausweissystem zeichnet sich durch die Unverfälschbarkeit aller Systemkomponenten aus. Um das vorgestellte System zu überwinden, muss ein Betrüger in den Besitz einer gültigen (registrierten) Karte und des biometrischen Merkmals, dessen Charakteristika auf der Karte gespeichert sind, kommen. D.h. der Diebstahl einer Karte allein verhilft nicht zum Zugang.

Die Manipulation der Ausweiskarte wird durch die holographische Speichertechnik wie oben beschrieben verhindert.

In dem Lesegerät wird ein Hardware-Schlüssel verwendet, mit dem die Informationen auf der Karte verschlüsselt sind, d.h. durch Unberechtigte nicht gelesen werden können. Dies geschieht wie ausgeführt durch Modulation des Referenzstrahls.

### **3 Zusammenfassung**

Zusammenfassend zeichnet sich das Ausweissystem für Hochsicherheitsanwendungen durch folgende drei maßgebliche Aspekte aus:

Das Ausweissystem der nächsten Generation stellt weitergehende Sicherheitsansprüche mittels nicht-digitaler, holographischer Speichertechnik sicher.

Das neue Ausweissystem berücksichtigt die Anforderungen an die Privatsphäre einer Person: Der Ausleseprozess darf nur bewusst durchgeführt werden können. Beim Auslesen der Karte dürfen Personen nur auf die für sie bestimmten Informationen Zugriff erhalten. Eine Datenkonsolidierung wird konzeptionell unterbunden.

Die wettbewerbsfähigen Kosten des neuen Ausweissystems konzentrieren sich vornehmlich auf die Leseinheit, so dass die Kosten pro Karte sehr gering ausfallen: Hierdurch wird die Einführung des Systems für einen großen Personenkreis ermöglicht.

### **4 Ausblick**

Wie bereits im Ansatz erwähnt, erlaubt das beschriebene Ausweissystem die Speicherung großer Datenmengen.

Damit lassen sich nicht nur Template von biometrischen Merkmalen festhalten, sondern es lassen sich umfangreiche biometrische Angaben speichern. Je größer die Basis an Referenzdaten, umso flexibler kann das System eingesetzt werden: Beispielsweise sind bei einigen Menschen die Papillaren auf den Fingerkuppen nur schwach ausgeprägt, so dass alternativ eine Überprüfung auf Basis der Iris oder des Gesichts vorgenommen werden kann. Auch können auf diese Weise ethischen oder religiösen Aspekten Rechnung getragen werden. Andererseits erlaubt der Einsatz mehrerer Biometrien einen präziseren Abgleich zwischen Person und Referenzdaten, der somit die Qualität des Sicherheitssystems erhöht.

Das Kartensystem erlaubt den Einsatz als sichere Speicherkarte, z.B. für Gesundheitsdaten: Die auf die Fläche einer Scheckkarten-Größe unterzubringende Speichermenge entspricht mehreren Hundert MBytes und ermöglicht das sichere Abspeichern von Kernspin- oder Röntgenaufnahmen. Diese können durch den Patienten in kontrollierter Weise von Behandlung zu Behandlung weitergereicht werden. Wiederholende Untersuchungen und

Kosten werden vermieden. Darüber hinaus können z.B. Anamnese-Daten in einem reservierten *Write-Once*-Bereich festgehalten werden, der physikalisch versiegelt und damit nicht mehr gelöscht werden kann.

Schließlich ist eine Kombination mit verschiedenen Technologien auf einer Karte denkbar. Z.B. könnte ein kombiniertes Ausweissystem über RFID-Technologie den Zugang zum Unternehmen „im Vorbegehen“ gewähren, während der Zugang zum Hochsicherheitstrakt einer Authentifizierung anhand des Abgleichs von biometrischem Merkmal und holographisch gespeicherten Referenzdaten bedarf. Hierdurch wird zugleich der Grundstein für eine Multifunktionskarte gelegt, die von verschiedenen Interessengruppen verwendet werden kann, ohne dass der einen Gruppe Zugriff auf die Daten der anderen Gruppe gewährt wird (logische und physikalische Trennung der Daten).

## Literatur

- [Schulz04] Christiane Schulzki-Haddouti: Alles auf eine Karte. In: c't, Heise (2004), Nr. 13, S. 46 (<http://www.heise.de/ct/04/13/046/>)
- [Bund04] Bundesministerium für Gesundheit und Soziale Sicherung: Informationen zur elektronischen Gesundheitskarte:  
<http://www.bmgs.bund.de/download/broschueren/a415.pdf>
- [Bund05] Informationen der Bundesdruckerei zum Personalausweis/Reisepass:  
[http://www.bundesdruckerei.de/de/iddok/2\\_1/index.html](http://www.bundesdruckerei.de/de/iddok/2_1/index.html)
- [Wiki05] Wikipedia. Die freie Enzyklopädie: Biometrie.  
<http://de.wikipedia.org/wiki/Biometrie>
- [ICAO04] ICAO TAG MRTD/NTWG Technical Report Version 2.0: Development and Specification of Globally Interoperable Biometric Standards for Machine Assisted Identity Confirmation using Machine Readable Travel Documents:  
<http://www.icao.int/mrtd/biometrics/recommendation.cfm>
- [HaBi01] R. Hagen, T. Bieringer: Photoaddressable Polymers for Optical Data Storage. In: Advanced Matererials, WILEY-VCH Verlag GmbH (2001), Nr. 13/23, S. 1805 – 1810
- [Hari02] P. Hariharan: Basics of Holography. University Press Cambridge (2002) 1-2