

► ID-DOKUMENTE



www.bundesdruckerei.de



„BORDERS ARE THERE TO BE CROSSED“

*Sicherheit und Schutz
individueller Identität gehört
zu den Grundbedürfnissen
des modernen Menschen*

Was immer uns in der Welt bewegt, in welchem Radius wir agieren und zu welchen Welten wir uns Zugang verschaffen möchten - Motor und Zentrum kleiner und großer Aufbrüche ist unsere individuelle Identität. Einmalig, echt und unverwechselbar bestimmen und erfahren wir unsere persönlichen Grenzen - einmalig, echt und unverwechselbar möchten wir wahrgenommen werden, wenn wir reale Grenzen überwinden.

*Seit mehr als 125 Jahren
bürgt die Bundesdruckerei
für Sicherheit*

Die Sicherheit und der Schutz individueller Identität gehört zu den Grundbedürfnissen und Grundrechten des modernen Menschen. Sie mit den modernsten Mitteln der Hochsicherheitstechnologie zuverlässig zu dokumentieren und gegen alle denkbaren Angriffe von Außen zu schützen, war und ist die wesentliche Aufgabe und das höchste Ziel unserer Arbeit in der Bundesdruckerei.

Seit mehr als 125 Jahren bürgen wir für Sicherheit und sind mit und an den permanent gestiegenen nationalen und internationalen Ansprüchen beständig gewachsen. Heute schließt die Bundesdruckerei den Kreis verlässlicher Identitätssicherung von der Herstellung hochsicherer Identitäts-Dokumente (ID-Dokumente) bis zur Entwicklung modernster Verfahren zur Identifizierung, Authentifizierung und Verifikation von Personen- und Dokumentendaten.

SICHERHEIT IST UNSER KERNGESCHÄFT

*Unsere ID-Dokumente zählen
zu den sichersten der Welt*

► In zahlreichen nationalen und internationalen Projekten haben wir dazu beigetragen, dass sich Menschen rund um den Globus sicher und frei bewegen können. Unsere ID-Dokumente zählen zu den sichersten der Welt. Technologisch setzen unsere Produkte und Lösungen innovative Maßstäbe. Und in der Entwicklung hochsicherer ID-Systeme gehören wir zu den wenigen global anbietenden Unternehmen, die nicht nur den Anspruch, sondern auch die Erfahrung haben, um ganzheitlich konzipierte Sicherheitsstrategien über die gesamte ID-Prozesskette kompetent und verlässlich steuern zu können.

*Identität ist mit allen
Mitteln zu schützen*

Ein wesentlicher Motor unseres Erfolges ist das frühzeitige Erkennen und Aufgreifen veränderter Sicherheitsanforderungen. Mit dem Aufbau des ersten deutschen Trust-centers haben wir auf die wachsende Bedeutung von Public-Key-Infrastrukturen (PKI) und elektronischen Signaturen reagiert. Mit der Entwicklung des EU-Kartenführerscheins konnten wir hinsichtlich der eingesetzten Sicherheitsmerkmale und Materialien weltweit neue Standards definieren. Und mit der Generalunternehmerschaft im initialen Einführungsprozess des europäischen ePasses in Deutschland ist es uns gelungen, neueste Verfahren zur Sicherung und Weiterverarbeitung biometrischer Daten im gesamten ID-Prozess abzubilden und umzusetzen.

Identität ist eines der wichtigsten Güter, das wir Menschen besitzen. Um sie mit allen zur Verfügung stehenden Mitteln abzusichern, gilt es immer wieder, technologische Grenzen zu überwinden und neue Zukunftsoptionen zu eröffnen.

Borders are there to be crossed – Dafür setzen wir uns ein. ◀



DER PASS

► Passe les Portes

*Der Pass dokumentiert die
Identität des Reisenden*

Schon seit Anfang des 13. Jahrhunderts begleitet uns eines der wichtigsten ID-Dokumente – der „passe port“ – eine in ihrer Geschichte 'zigfach modifizierte Berechtigung zum Durchschreiten von Türen, Schranken und Grenzen. Die Bedingungen und Anforderungen, die über die Jahrhunderte an die Sicherheit dieser Ausweisdokumente geknüpft wurden, belegen auch ein gewaltiges Stück internationaler Kultur- und Politikgeschichte.

Bedingt durch die zunehmende Globalisierung und wachsende Mobilität der Menschen, definiert die internationale Staatengemeinschaft mit Beginn des 21. Jahrhunderts ihre Anforderungen an die Unverwechselbarkeit und Sicherheit individueller Ausweisdokumente nochmals neu. Der Pass ist Beweis und Kontrollmedium gegenseitigen Vertrauens. Er dokumentiert die Identität eines Reisenden und erlaubt – zumindest auf Basis der neuesten ID-Verfahren – eine eindeutige Zuordnung zwischen der Person und ihrem Dokument. ◀

NATIONALE IDENTITÄTEN GLOBAL SICHERN

*ICAO empfiehlt die
internationalen
Sicherheitsrichtlinien*

► Jeder Staat muss sicher stellen, dass sich die in ihm beheimateten Bürger mit ihrem nationalen ID-Dokument innerhalb der Staatengemeinschaft frei und grenzüberschreitend bewegen können. Hierzu muss einerseits gewährleistet sein, dass der Bürger auf die Richtigkeit und Sicherheit seines Dokuments vertrauen und andererseits alle Länder der Welt das ausgestellte Reisedokument als verlässlichen Identitätsnachweis akzeptieren können.

Damit aber grundlegende Informationen, unabhängig von sprachlichen und kulturellen Unterschieden, weltweit verstanden, verarbeitet und automatisiert geprüft werden können, sind zahlreiche internationale Vereinbarungen und Standardisierungen notwendig. Die Rolle der Steuerung dieser Prozesse übernimmt die 1944 als Unterorganisation der Vereinten Nationen (UN) gegründete International Civil Aviation Organisation (ICAO). Ihre Empfehlungen münden in die Normierungsprojekte der International Organization for Standardization (ISO), in der über 150 Länder vertreten sind. ◀



HOCHSICHERHEITS- DOKUMENT PASS

*Sicher vor Fälschung
und Missbrauch*

► Im Prozess der Produktion nationaler Reisedokumente sind die Auftraggeber der Bundesdruckerei in der Regel die Ministerien einzelner Länder, die ihre hoheitliche Aufgabe der Bereitstellung international gültiger ID-Dokumente mit Unterstützung von einigen wenigen, berechtigten Partnerunternehmen erfüllen.

Grundsätzlich muss jedes hoheitliche Personaldokument so ausgelegt sein, dass es sicher gegen Fälschungen oder Verfälschungen geschützt ist und den Missbrauch echter Dokumente durch unberechtigte Personen nachhaltig erschwert bzw. ausschließt.

Gleichzeitig ist darauf zu achten, dass das optische Erscheinungsbild den kulturellen, historischen und religiösen Gegebenheiten eines Landes entspricht und sich gestalterisch in das Design bestehender Dokumentenfamilien einfügt. Alle funktionalen Anforderungen – Widerstandsfähigkeit gegen Chemikalien, Tauglichkeit für Einsatzbereiche von -10° bis +50°C und Lagertemperaturen von -35° bis +85°C, weltweite Interoperabilität, keine Einschränkung der Funktionalität bei Deformation, nicht giftig, maschinenlesbar von 5% bis 95% relativer Luftfeuchtigkeit, hohe Lichteuchtigkeit, gesicherte Lieferketten – müssen mit den mechanischen, elektrischen und elektronischen Prozessen abgestimmt sein.

Zur Verbesserung des internationalen Grenzverkehrs hat die ICAO seit dem Jahr 2001 spezifische Empfehlungen zur zusätzlichen Integration biometrischer Daten in international gültigen Reisedokumenten ausgesprochen. Diese wurden von den Ländern der EU aufgenommen, spezifiziert und als verbindliche Rechtsgrundlage beschlossen. ◀

DER DEUTSCHE ePASS

► Die Erfassung der biometrischen Daten, an der die Bürger, die zuständigen Passbehörden, die Botschaften und die Auslandsvertretungen der einzelnen Länder beteiligt sind, gliedert sich in der Europäischen Union in zwei, zeitlich versetzte Einführungsphasen.

*Die Einführung des ePasses
in Deutschland ist
in zwei Phasen unterteilt*

In Phase I (in Deutschland im November 2005 gestartet) werden nur das Lichtbild des Antragstellers und die personenbezogenen Daten, in Phase II (für Deutschland geplant ab 2007) die zusätzlichen Daten von zwei Fingerabdrücken als biometrische Merkmale erfasst und auf einem im Dokument integrierten Chip gespeichert. Mit dieser technologischen „Aufrüstung“ bleiben selbstverständlich alle bewährten Sicherheitsmerkmale wie das Identigram® mit seinem Holographic Shadow Picture (HSP® - holographisches Schattenbild), die kinematischen Bewegungsstrukturen, die holographische Wiedergabe der maschinenlesbaren Zeile (MRZ - Machine Readable Zone), die maschinell prüfbar sind, die Strukturen und Oberflächenprägungen sowie die drucktechnischen Sicherheitsmerkmale, wie Guillochen, Mikroschriften, Irisdruck, UV-Druck, und materialtypische Merkmale wie Wasserzeichen oder taktile Laserung, unverändert erhalten.

*Die Bundesdruckerei ist
Hersteller des
deutschen ePasses*

Über die eingespielten Verfahren und Prozesse ihrer Lieferkette konnte die Bundesdruckerei die neuen technischen Herausforderungen ebenso problemlos meistern wie die angeforderten Unterstützungsleistungen im Bereich infrastruktureller Anpassungen im behördlichen Datenerfassungsprozess. ◀



► Der deutsche elektronische Reisepass seit 1. November 2005

DIGITALE SICHERHEITS- MERKMALE DES ePASS

► Für die Sicherheit des europäischen ePasses sind zwei Aspekte von entscheidender Bedeutung: Die Sicherheit des kontaktlos betriebenen Chips mit den darauf gespeicherten Daten und der sichere Umgang mit den personenbezogenen Daten während der Personalisierung.

Radio Frequency (RF) – Chip

*Persönliche Daten auf
dem Chip sind gegen
unberechtigtes Auslesen oder
Verändern geschützt*

Um eine verlässlichere Bindung zwischen Dokument und Dokumenteninhaber gewährleisten zu können, wird der ePass mit einem zertifizierten Radio-Frequency (RF) – Sicherheitschip mit kryptographischem Koprozessor ausgestattet. Neben den bisher üblichen Passdaten können auf ihm auch biometrische Merkmale abgespeichert werden. Die grundlegenden technischen Spezifikationen der für den Reisepass vorgesehenen RF-Chips wurden von der ICAO standardisiert.

Auf dem Weg, den die persönlichen Daten eines Antragstellers vom Ort ihrer Erfassung über die Integration ins Dokument bis zum Zeitpunkt eines erneuten Auslesens – zum Beispiel am Grenzkontrollpunkt – zu überwinden haben, greifen zahlreiche, hochkomplexe Mechanismen, um die Daten gegen unberechtigtes Auslesen oder Verändern zu schützen.

Digitale Signaturen

Eine wesentliche Schutzfunktion für die Integrität und Authentizität der im RF-Chip gespeicherten Daten erfüllen digitale Signaturen. Jedes Land, das sich zu den Grundsätzen einer weltweit verbindlichen Public Key Infrastruktur (PKI) bekennt, erzeugt zur Sicherung seiner nationalen Reisepässe eine zweistufige PKI, die aus nur einer Country Signing CA (Certification Authority) und mindestens einem Document Signer besteht. Document Signer sind dabei ausschließlich die zum Signieren digitaler Dokumente berechtigten Stellen (z. B. Produzenten von ID-Dokumenten), die von der Country Signing CA entsprechend zertifiziert werden. Damit wird sicher gestellt, dass die signierten Daten ausschließlich von berechtigten Stellen erzeugt und danach nicht mehr verändert werden können. Auf diese Weise wird jede Form unechter oder manipulierter Daten erkennbar.

Zugriffsschutz

Schon in den herkömmlichen Passdokumenten sind alle personenbezogenen Daten – also Name, Geburtsdatum und Geschlecht – in einer maschinenlesbaren Form auf der Datenseite des Reisepasses verfügbar. Nur das Gesichtsbild war bislang nicht in die sogenannte Machine Readable Zone (MRZ) integriert, sondern auf die Datenseite des Dokuments gedruckt. Im geschlossenen Zustand des Passbuches hatte damit auch bei den herkömmlichen Dokumenten niemand Zugang zu den verzeichneten Daten. Ein Auslese- oder Kontrollvorgang konnte nur dann vorgenommen werden, wenn der Passinhaber berechnete Personen persönlich autorisierte, zum Beispiel im Rahmen einer Grenzkontrolle.

Auch für die im RF-Chip gespeicherten Daten gilt diese grundsätzliche Form des Zugriffsschutzes. Um jede Form eines unrechtmäßigen Auslesens der Daten oder ein Belauschen der Kommunikation zu verhindern, greift die sogenannte Basic Access Control. Der elektronische Zugriffsschutz gestattet dem (Pass-)Lesegerät nur dann Zugang zu den gespeicherten Daten, wenn tatsächlich ein optischer Kontakt zur Datenseite des Reisepasses vorhanden ist und sich das Lesegerät gegenüber dem RF-Chip als berechtigt „ausweisen“ kann. Hierfür ist ein geheimer Zugriffsschlüssel notwendig, der sich aus diversen Daten der MRZ des Reisepasses berechnet.

In der zweiten Stufe des ePasses, in der die zusätzliche Speicherung von Fingerabdruckdaten des Passinhabers auf dem RF-Chip geplant ist, wird dieser Zugriffsschutz nochmals erweitert. Dabei spezifiziert die Extended Access Control einen Public-Key Authentisierungsmechanismus, der nur mit einem speziell für das Lesegerät zertifizierten Schlüsselpaar und einem vom RF-Chip verifizierbaren Zertifikat gestartet werden kann. Auf welche Daten ein Lesegerät zugreifen darf, liegt dabei ausschließlich in der Entscheidungsbefugnis des den Pass ausstellenden Landes. Von einem – in dem die Zugriffsrechte exakt definiert sind – geschlossenen Passbuch können auch im Rahmen der Extended Access Control keine Daten ausgelesen werden, weil die Basic Access Control weiter vorgeschaltet bleibt.

Verschlüsselung

Grundsätzlich wird nach der erfolgreichen Durchführung der Basic Access Control die Kommunikation zwischen Lesegerät und RF-Chip mit 112-Bit-Triple-DES verschlüsselt und ist somit prinzipiell gegen unberechtigtes Abhören geschützt. Die nachträgliche Entschlüsselung eines Vorgangs über einen sogenannte Brute-Force-Angriff (Ausprobieren aller möglichen Schlüssel) würde, wenn überhaupt möglich, extrem viel Zeit und hochkomplexe Hard- und Software-Systeme voraussetzen. Die derzeit auf EU-Ebene diskutierten Spezifikationen der Extended Access Control sehen dennoch vor, nach dem erfolgreichen Durchlauf der Basic Access Control einen noch stärkeren Sitzungsschlüssel aufzubauen, der über Public-Key-Mechanismen (PKI) erzeugt werden wird.

Dokumentenbindung

Die Fälschungssicherheit stand auch bei den herkömmlichen Passdokumenten nicht in Frage. Was durch die Integration von biometrischen Merkmalen in den RF-Chip eines ePasses jedoch bereits heute erreicht wurde und mit der Speicherung von Fingerabdrücken weiter ausgebaut werden wird, ist die Möglichkeit zur Herstellung einer eindeutigen Verbindung zwischen Dokument und Dokumenteninhaber. Über spezielle Gesichtserkennungs- bzw. Fingerprintsysteme können die gespeicherten Daten eines ePasses direkt mit den „live“-Daten des sich ausweisenden Reisenden verglichen werden. Ein Missbrauch echter Dokumente durch unberechtigte Personen wird damit verhindert. ◀

*Die Speicherung der
Fingerabdrücke ermöglicht
eine eindeutige Verbindung
zwischen Dokument
und Dokumenteninhaber*



DER INTERNATIONALE PASS

► Über Projekte zur Produktion hochsicherer nationaler ID-Dokumente hinaus, bietet die Bundesdruckerei auch im Rahmen internationaler Vorhaben zahlreiche Lösungen, die den unterschiedlichen Situationen in den Zielländern gerecht werden.

Im Rahmen der ICAO-Empfehlungen ist die Position des RFID-Chips im Reisepass nicht vorgegeben. Damit sind viele unterschiedliche Szenarien und präzise Anpassungsverfahren auf die national vorhandenen Infrastrukturen oder andere Vorgaben nötig und möglich.

Flexible Flat Link (FFL)[®] – die Lösung für hochfeste Bindungen

Eine unmittelbare Verbindung zwischen dem RF-Chip, der die biometrischen Daten elektronisch speichert, und der Datenseite oder -karte des Passes, die die biometrischen und biographischen Daten optisch speichert, hat einige Vorteile. Besteht die Datenseite vollständig aus Kunststoff, ist sie optimal gegen äußere Einflüsse wie Wasser, Schmutz, Verbiegungen etc. geschützt und selbst bei Zerstörung des papierbasierten Passbuchs, bleiben alle Daten erhalten.

*FFL[®]-Lösung setzt neue
Maßstäbe für die Haltbarkeit
und Sicherheit
von Reisepässen*

Die von der Bundesdruckerei entwickelte Lösung für die hochfeste Bindung einer Polycarbonat-Datenseite im Reisepass, die Flexible Flat Link (FFL)[®], basiert auf einem speziellen Kunststoffverbund, der eine extrem hohe Reißfestigkeit aufweist und – anders als andere am Markt erhältliche Trägermaterialien – der Biegebeanspruchung beim Öffnen und Schließen des Passes über viele Jahre absolut zuverlässig standhält. Darüber hinaus bietet FFL[®] zusammen mit den Polycarbonatfolien eine außerordentlich hohe Verbundhaftung, sodass eine Zerlegung des Passes in einzelne Folien ausgeschlossen ist. Einband, Passbuch, Datenseite und der empfindliche Chip müssen im Ernstfall extreme Belastungen unbeschadet überstehen. Mit der FFL[®]-Lösung, für die die Bundesdruckerei spezielle Prozessschritte und Werkzeuge entwickelt hat, sind neue Maßstäbe für die Haltbarkeit und Sicherheit von Reisepässen gesetzt worden.

*Eigenentwickelte
eFlexCover-Lösung gewähr-
leistet eine sichere
dezentrale Personalisierung*

eFlexCover für die dezentrale Personalisierung

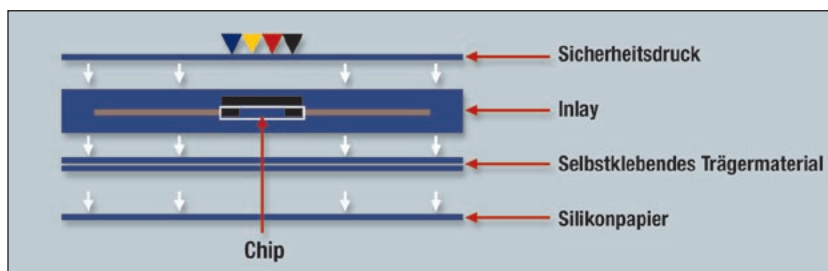
In einigen Ländern gibt die vorhandene Infrastruktur eine dezentrale Personalisierung der Reisepässe vor oder der RF-Chip muss sich an ein bestehendes Dokumentendesign anlehnen. Für solche Anforderungen stellt die Bundesdruckerei die eigenentwickelte eFlexCover-Lösung bereit. Hierbei wird das Inlay mit dem RF-Chip sowohl durch einen speziellen Nähvorgang als auch durch einen nicht zerstörungsfrei trennbaren Kleber mit dem Deckenmaterial des Passbuchs verbunden. Die Personalisierung der Datenseite kann durch die bewährten Inkjet-Verfahren erfolgen.

Damit werden auch die Missbrauchsmöglichkeiten im Falle von Diebstahl von Blanko-Pässen erheblich erschwert.

*RF-Chip integriert
in einen Aufkleber*

ePass-Sticker

Eine weitere Lösung zur Nachrüstung vorhandener maschinenlesbarer Passdokumente, die jenseits der biometrischen Komponente ICAO-konform sind und weiter verwendet werden sollen, bietet die von der Bundesdruckerei angebotene Lösung des sogenannten „ePass-Stickers“. Hier wird der RF-Chip in einen Aufkleber integriert und kann wahlweise auf die inneren Vorsatzseiten oder die Rückseite der Datapage aufgeklebt werden. Dieses Verfahren ist allerdings von der Art der Bedruckung des Untergrunds (z.B. Intaglio) ebenso abhängig wie von der Stärke der Datenseite und kann deshalb nicht in jedem Fall realisiert werden.



► ePass Sticker

*Sichere Verschlüsselung
des Chips im ePass*

Die Chip-Technologie

Die in den deutschen und zahlreichen internationalen ePässen eingesetzten Hochsicherheits-Chips werden der Bundesdruckerei von ihren Technologiepartnern Infineon Technologies und Philips Semiconductors zugeliefert. Beide Unternehmen verfügen über große Erfahrungen in hoheitlichen und privatwirtschaftlichen Hochsicherheitsbereichen.

*Die Chiptechnologien
entsprechen allen Standards*

Über 50 hochspezifische Sicherheitsmechanismen und alternative Signaturverfahren – im deutschen ePass wird über ECDSA (Elliptic Curve Digital Signature Algorithm), in einigen internationalen Dokumenten über RSA* verschlüsselt – schützen die in den Chips gespeicherten Daten. Schätzungen gehen davon aus, dass rund eine Million Standard-PC's über eine Million Jahre im „Trial & Error“-Verfahren parallel arbeiten müssten, um die digitalen High-Security-Schutzwälle um die ePass-Daten durchbrechen zu können. ◀

* Das RSA-Kryptosystem ist ein asymmetrisches Kryptosystem, d. h. es verwendet verschiedene Schlüssel zum Ver- und Entschlüsseln. Es ist nach seinen Erfindern Ronald L. Rivest, Adi Shamir und Leonard Adleman benannt



DIE ID-KARTE

► Viele Staaten händigen zusätzlich zum Reisepass zahlreiche weitere Dokumente aus, die das öffentliche Leben der Bürger und der Staatsorgane erleichtern sollen. Die ID-Karte ist eines der international gebräuchlichsten Mittel, um sich zu legitimieren und wird als digitaler Personalausweis zur Unterstützung der gestiegenen Sicherheitsanforderungen im eGovernment und eBusiness eingesetzt. Um den gewünschten Funktionen (Authentisierungs- und Signaturfunktion, höhere Fälschungssicherheit, Integration biometrischer Merkmale) gerecht zu werden, muss die ID-Karte über einen integrierten Chip verfügen.

Die zentrale und dezentrale Personalisierung von ID-Karten

Im einem zentralen Personalisierungsszenario wird die ID-Karte nur an einer oder wenigen ausgewählten Stellen produziert und kann in der Regel nicht am Ort der Beantragung personalisiert werden. In einem dezentral organisierten Personalisierungsprozess werden die Karten als nummerierte Kartenkörper an unterschiedliche hoheitliche Ausgabestellen geliefert und können mit bestimmten Druckern vor Ort optisch und elektrisch personalisiert werden. Allerdings sind dezentrale Systeme nur dann erfolgreich, wenn im Land tragfähige Infrastrukturen (Telefon, Post, Strassen) vorhanden sind.

Die Bundesdruckerei liefert Hybridkarten, die beiden Funktionalitäten gerecht wird. Mittels eines „live“ geladenen Zertifikats, werden hier bestimmte elektronische Dienste (single sign on für emails, etc.) umgehend nutzbar. Um die Marktfähigkeit solcher Optionen weiter voranzutreiben, kann die Bundesdruckerei mit dem Know-how ihres Trustcenter zum Aufbau nationaler Trustcenter beitragen. ◀



13.	9.	10.	11.	12.
A1		—	—	—
A		—	—	—
B		13.08.82	—	—
C1		13.08.82	—	171
C		—	—	—
D1		—	—	—
D		—	—	—
BE		13.08.82	—	—
C1E		13.08.82	—	—
CE		13.08.82	12.08.14	79 (C1E > 12000kg, L ≤ 3)
D1E		—	—	—
DE		—	—	—
M		15.08.80	—	—
L		15.08.80	—	174, 175
T/S	—	13.08.82	—	181
12.	—	—	—	—

14. (10.)

1. Name 2. Vorname
3. Geburtsdatum und -ort
4a. Ausstellungsdatum
4b. Ablaufdatum
4c. Ausstellungsbehörde
5. Führerscheinnummer
9. Fahrerlaubnisklasse
10. Erstellungsdatum
11. gültig bis 12. Beschränkungen/Zusatzangaben

► Deutscher EU-Kartenführerschein

DER EU-KARTENFÜHRERSCHEIN

*Richtlinien sollen
Führerscheine in
der europäischen Union
vereinheitlichen*

► Die Akzeptanz der alten, national unterschiedlich gestalteten Führerscheine wird außerhalb der jeweiligen Landesgrenzen immer geringer. Der überall in der europäischen Union akzeptierte und gültige EU-Kartenführerschein bildet die einzig rechtsverbindliche Voraussetzung, um einen internationalen Führerschein zu beantragen.

*Moderner und sicherer
Führerschein im praktischen
Scheckkartenformat*

Zum gegenwärtigen Zeitpunkt gibt es europaweit ca. 110 gültige Führerscheinvarianten. Die mit dem Ziel eines einheitlichen Layouts erstmals 1991 erlassene Richtlinie (91/439/EWG) wurde in den letzten Jahren mehrfach geändert und überarbeitet. Die Überarbeitungen bzw. Neufassungen basieren zum einen auf technischen Weiterentwicklungen der Dokumente im Hinblick auf ihre Fälschungssicherheit und zum anderen auf den Anspruch zur Harmonisierung der Fahrzeugklassen im EU-Raum. Aktuell ist eine neue Richtlinie in Bearbeitung, die eine Begrenzung des Gültigkeitszeitraumes auf zehn Jahre und die Integration eines elektronischen Datenspeichers und weitere Sicherheitsmerkmale vorsieht. Parallel dazu wird der Aufbau einer dezentralen europäischen Datenbank zur Erhöhung der Verkehrssicherheit und zur Vermeidung von Missbrauch vorbereitet.

*Bundesdruckerei-Know-how
auch international gefragt*

Seit 1999 können deutsche Verkehrsteilnehmer bei den regional zuständigen Fahrerlaubnisbehörden den modernen Führerschein im praktischen Scheckkartenformat beantragen. Die Herstellung der Kartenkörper und die Personalisierung der Dokumente erfolgt zentral bei der Bundesdruckerei. Über 27 Millionen EU-Kartenführerscheine wurden in den Berliner Produktionshallen allein für deutsche Fahrer und Fahrerinnen produziert. Doch auch im Ausland ist das Know-how „Made in Berlin“ gefragt. Neben den bundesdeutschen Führerscheinen produziert die Bundesdruckerei derzeit die portugiesischen, isländischen und litauischen Fahrerlaubnisse. ◀



DER VISUM-STICKER

► Ebenso wie im ePass-Sticker könnten auch international gültige Visa mit der Speicherung biometrischer Komponenten ergänzt werden. Hierzu werden derzeit in der Europäischen Union erste Überlegungen angestrengt, die den Einsatz biometrischer Abgleichmethoden an Schengen-Grenzen im Rahmen der Kontrolle elektronischer Reisepässe und auf Basis eines zentralen Visa-Informationssystems vorsehen.

Die Integration biometrischer Daten kann auch in diesem Kontext dazu beitragen, dass eine verlässlichere Verbindung zwischen dem Inhaber und dem Visum bzw. dem Aufenthaltstitel hergestellt werden kann. Langfristig ist auch die Anbindung an internationale Datenbanken denkbar.

*Ziel: internationalen
Grenzverkehr sicherer und
komfortabler gestalten*

Sowohl für die Visumerteilung, bei der die Information, ob einem Antragsteller bereits zu einem früheren Zeitpunkt ein Visum erteilt oder abgelehnt wurde, wichtig ist, als auch für Grenzkontrollen entstehen über die Nutzung der Möglichkeiten eines maschinellen Abgleichs von Passinhaber und Dokument auf Basis biometrischer Daten neue Optionen, um den internationalen Grenzverkehr für alle Bürger sicherer und komfortabler zu gestalten. ◀

BEWÄHRTE SICHERHEIT

► Allgemeine Sicherheitsmerkmale

klassisch
optisch
maschinenlesbar

Alle ID-Dokumente sind jenseits ihrer digitalen Sicherheitsmerkmale mit zahlreichen klassischen, optischen und maschinenlesbaren Sicherheitsfunktionen ausgestattet, die sich über viele Jahre bewährt haben bzw. beständig verbessert und verfeinert wurden. Die Bundesdruckerei ist in der Lage, alle bekannten Sicherungsmechanismen zum Schutz personenbezogener Daten und zur Gewährleistung verlässlicher Fälschungssicherheit anzubieten.

Generell wird bei der Klassifizierung der Sicherheitsmerkmale in mindestens drei Stufen unterschieden:

*Ohne technische
Hilfsmittel zu erkennen*

Sicherheitsmerkmale der ersten Ebene bezeichnen alle Sicherheitsmerkmale, die ohne technische Hilfsmittel zu erkennen sind, zum Beispiel die Taktilität des Stichtiefdruck, das Wasserzeichen, der Sicherheitsfaden, die holographischen Elemente, optisch variable Farben oder das Durchsichtsregister.

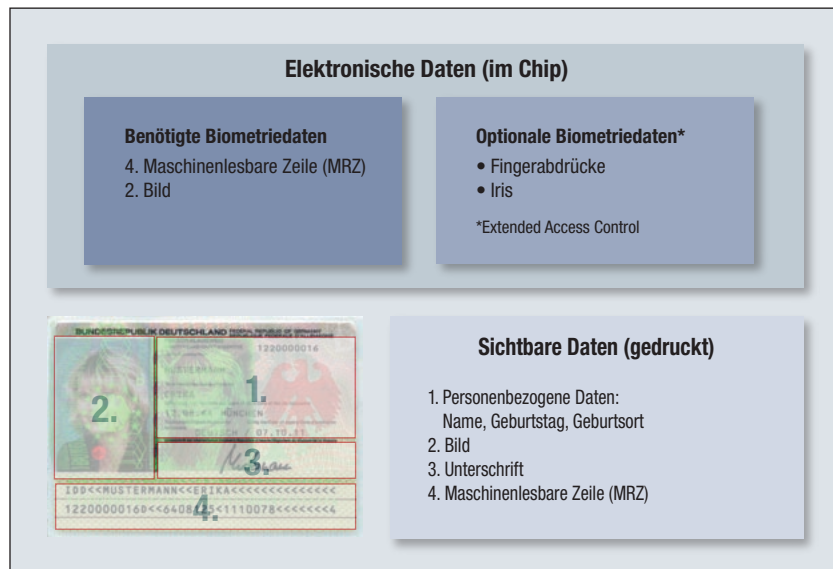
*Ausschließlich mit
spezifischen Hilfsmitteln
zu erkennen*

Sicherheitsmerkmale der zweiten Ebene bezeichnen all jene Merkmale, die ausschließlich mit spezifischen Lesegeräten oder anderen technischen Hilfsmitteln zu erkennen sind, zum Beispiel Fluoreszenzen, Metamerie, Mikroschrift, digitale Wasserzeichen oder die Maschinenlesbare Zeile (MRZ).

*Nur forensisch
auswertbar*

Sicherheitsmerkmale der dritten Ebene bezeichnen Sicherheitsmerkmale, die nur einem sehr eingeschränkten Personenkreis bekannt und in der Regel nur forensisch auszuwerten sind.

Die elektrischen Sicherheitsmerkmale werden nochmals in drei Stufen klassifiziert. Den Sicherheitsanforderungen der Stufe 1 genügen dabei solche Sicherheitsmerkmale, die keine oder nur eine einfache Authentisierung mit wenigen Überprüfungen der Systemintegrität erfordern (z. B. bei isolierten, portablen Lesegeräten). Für die Sicherheitsanforderungen der Stufe 2 muss der Entwurf eines Schlüsselmanagements vorliegen, um starken Angriffen auf allen Ebenen widerstehen zu können. Entsprechende Lesegeräte verfügen somit über Aktualisierungseinrichtungen zur Integration jeweils neuer Schlüsselgenerationen. Allein spezifische, auf die jeweilige Anwendung zugeschnittene Chipkartenmodelle, die weder unberechtigt ausgelesen noch manipuliert werden können, genügen den Sicherheitsanforderungen der Stufe 3.



Sicherheit im Papier

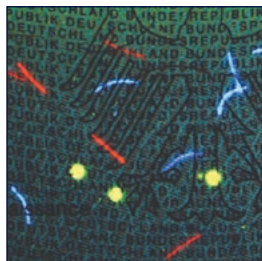
Das für die Herstellung von Reisepässen und anderen ID-Dokumenten notwendige Sicherheitspapier, in dem unterschiedliche Sicherheitsmerkmale enthalten sein können, muss frei von Aufhellern sein, sollte über einen hohen Baumwollanteil verfügen und mehrstufige Wasserzeichen ermöglichen. Zusätzlich darf das Material nicht die Einbettung von Fäden oder Fensterfäden, Planchetten oder Melierfasern mit unterschiedlichen UV-Eigenschaften erschweren und muss gegen Attacken durch chemische Reagenzien abgesichert sein.



► *Mehrstufiges Wasserzeichen*



► *Eingebetteter Sicherheitsfaden (UV-fluoreszierend)*



► *Meliefasern und Planchetten unter UV-Beleuchtung*

► **Sicherheitsmerkmale/Druck**

Sicherheit in Farben und Drucktechniken

Die Bundesdruckerei verfügt über langjährige Erfahrungen und Kompetenzen im Einsatz aller Druckverfahren, die im Bereich des Wertdrucks eine Rolle spielen. Zusätzlich kann sie jederzeit auf das Know-how ihrer hauseigenen Farbenreiberei zurückgreifen, die als interner Ansprechpartner bei der Entwicklung oder dem Einsatz neuester Sicherheitsfarben eine wichtige Rolle spielt. Die richtige Auswahl der Verfahren, das Know-how der Funktionalitäten der Sicherheitsmerkmale und fundierte Kenntnisse von Wechselwirkungen sind für die Qualität von ID-Dokumenten von zentraler Bedeutung.

Stichtiefdruck

*Taktil wahrnehmbares
Sicherheitsmerkmal*

Seit Beginn des industriellen Sicherheitsdrucks ist das Intaglio-Verfahren (Stichtiefdruck) bekannt und erprobt. Dabei erhält die Druckform tiefliegende Linienstrukturen, die das Motiv bilden und durch die Tiefenvariabilität verschiedene echte Halbtöne erzeugen. Die hochviskose Druckfarbe wird über eine erwärmte Druckform aufgetragen, wobei der hohe Pressdruck auf dem Papier ein hochstehendes Druckbild bildet, das taktil wahrnehmbar ist. Bestimmte Sicherheitsmerkmale, wie der Kippeffekt oder, sind nur mit diesem Verfahren möglich. Über die Einführung der Orlof-Technik ist eine zusätzliche Einfärbung der Druckform in bis zu drei Farben möglich, so dass in einer Linie entsprechend dem Farbschnitt versatzfrei ein Wechsel der Farbe stattfinden kann.

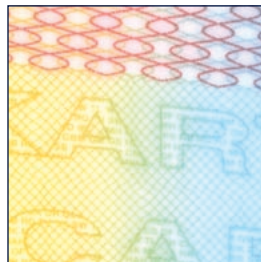


► *Kippeffekt (latent image)*

*Sicherheitsdruck setzt ein
hohes Know-how voraus*

Offset

Der Offsetdruck ist ein Flachdruckverfahren, bei dem druckende und nicht druckende Elemente in einer Ebene liegen und das Druckbild durch Abstoßungseffekte zwischen Fett (Druckfarbe) und Wasser (Feuchtmittel) erzeugt wird. Im Sicherheitsdruck werden, anders als in kommerziellen Druckverfahren, jedoch keine Prozessfarben (4c), sondern diverse Sonderfarben eingesetzt und die Motive werden nicht durch konventionelle Rasterpunkte, sondern durch die Auflösung in Linien und Spezialraster erzeugt. Obgleich im Offset-Bereich – anders als beim Intagliodruck – entsprechende Maschinen frei verfügbar sind, werden langjährige Erfahrungen im Irisdruck, in der Verarbeitung und Erzeugung der Druckformen und im Umgang mit spezifischen Software-Produkten und hochauflösenden Druckvorstufen-Equipments benötigt, um die angestrebte Sicherheitsqualität zu erreichen.



► *Irisdruck (rainbow printing)*

Letterpress

Letterpress ist ein Hochdruckverfahren, bei dem die druckenden Elemente erhaben sind. Der indirekte Hochdruck ermöglicht – neben dem simultanen Drucken von Farben auf einen Zylinder und von dort auf das Papier – auch den Einsatz von Farben mit unterschiedlichen Reagenzien und erzeugt ein unverwechselbares Druckbild (Quetschrand), das die Fälschungserkennung unterstützt.

Siebdruck

Im Siebdruck (Durchdruckverfahren) werden die verwendeten Farben, auch solche mit großen Pigmenten wie OVI oder Silberpasten, durch unterschiedlich gerasterte Siebe gedruckt, was durch den potenziell hohen Farbauftrag eindeutige Merkmale des Erscheinungsbildes und irisierende Effekte ermöglicht.

Lumineszenz

Neben den direkt in das Papier eingebrachten fluoreszierenden Fasern, können auch einzelne Motive für die Bedingungen normaler Beleuchtung unsichtbar gemacht werden. Hierzu werden den eingesetzten Farben verschiedene Fluoreszenzen beigemischt, die erst unter spezieller Beleuchtung (UV) sichtbar werden. Für den Sicherheitsdruck interessant sind dabei auch Fluoreszenzen, die im nahen IR-Bereich emittieren.



► VISOTEC UV-Bild

Metamerie

Metamerie bedeutet, dass Farben unter verschiedenen Beleuchtungsquellen unterschiedlich reagieren. Im Sicherheitsdruck wird Metamerie immer dann eingesetzt, wenn sich Motive unter Weißlicht nicht aus der Umgebungsfläche abheben, sondern erst unter speziellen Beleuchtungseffekten (z. B. Grünlicht oder Infrarotlicht) hervortreten sollen. Dieser Effekt wird insbesondere zur Unterstützung der Lesbarkeit von maschinenlesbaren Zeilen (MRZ) eingesetzt.



► VISOTEC IR-Bild

► Sicherheitsmerkmale/Farben-Muster

Optisch variable Farben (OVI)

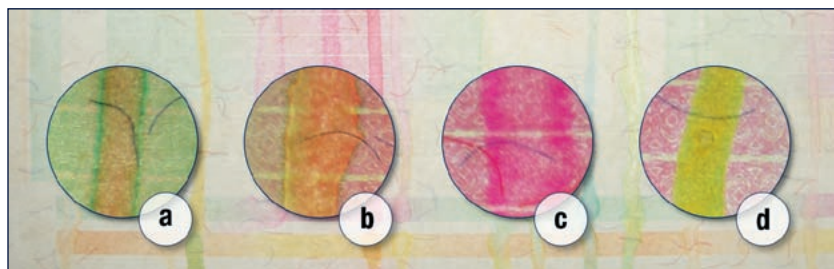
Durch variierende Reflektionen aus unterschiedlichen Winkeln führt der Einsatz von OVI-Farben beim Kippen des Dokuments zu markanten Farbumschlägen, die seit langem zur Fälschungssicherheit von Banknoten eingesetzt werden. Dabei erscheint eine Farbe in der Frontalansicht z. B. violett und verändert sich unter einem anderen Betrachtungswinkel ins grün-bräunliche.



► *Optisch variable Farbe*

Lösungsmittellösliche Farben

Spezielle lösungsmittellösliche Farben reagieren auf Manipulationsversuche durch Säuren, Laugen, Alkohole, Erdölderivate, Tintenkiller oder Bleichmittel. Damit kann das Verfälschen von Einträgen auf Daten- oder Visa-Seiten weitestgehend ausgeschlossen werden.



► *Manipulationsversuche mit: a: Säure, b: Lauge, c: organischem Lösungsmittel, d: Bleichmittel*

Klassische Sicherheitsmuster

Um die im Sicherheitsdruck verwendeten Muster in hoher Qualität erzeugen zu können, bedarf es unterschiedlicher Spezialsoftware und hochauflösender Ausgabegeräte, die ausschließlich Sicherheitsdruckereien zur Verfügung stehen.

Als führendes Traditionsunternehmen im Sicherheitsdruck verfügt die Bundesdruckerei über bewährte Netzwerke zu spezialisierten Geräte- und Software-Anbietern. Die derzeit eingesetzten Ausgabegeräte ermöglichen Auflösungen bis zu 10.160 dpi.

Mikroschrift

Schriften, die ohne technische Hilfsmittel (Lupe, MRZ-Lesegerät) nicht mehr lesbar sind, werden als Mikroschrift bezeichnet. Die Bundesdruckerei bedient sich der prozessbedingt jeweils kleinsten Schriftgrößen, die positiv (Schrift auf weißem Grund) oder negativ (im Hintergrund ausgespart) gesetzt werden und in Kombination mit Bildern oder Linienmodulationen verwendet werden. Fälschungen via Kopierer sind damit praktisch ausgeschlossen.



► Positive und negative Mikroschrift

Guillochen

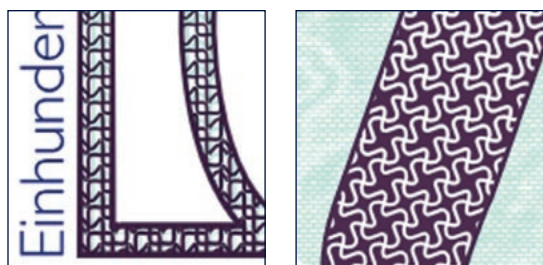
Die sogenannten Guillochen sind feine Linien, die auf Basis mathematischer Funktionen zu meist mehrfarbigen Mustern und Formen verarbeitet werden und sowohl positiv als auch negativ erzeugt werden können.

Bei kopierten Dokumentenfälschungen können gleichzeitig verwendete Positiv- und Negativ-Guillochen nicht adäquat wiedergegeben werden, so dass leicht erkennbare Unschärfen im Linienverlauf entstehen.



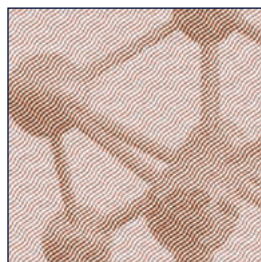
► *Negativ- & Positiv-Guillochen*

In Kombination mit fraktalen Mustern oder unterschiedlichen Tonwerte eines Bildes (Linienraster) kann zudem eine große Variantenbreite von Linienmodulationen und Reliefs, die dem Motiv einen dreidimensionalen Charakter verleihen, erzeugt werden.



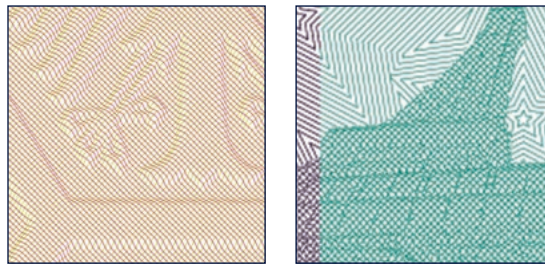
► *Linienmodulation*

► *Fraktale Muster*



► *Linienmodulation in Kombination mit einem Bild*

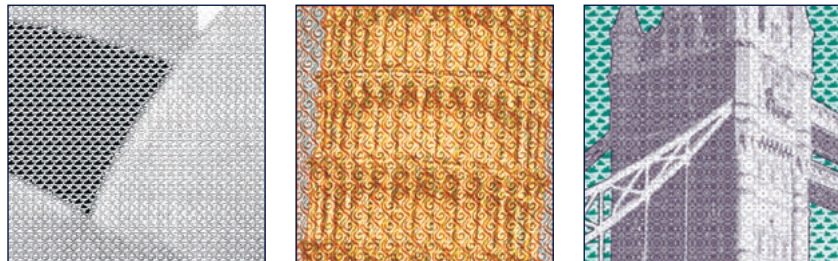
Durch die Regelmäßigkeit der Strukturen, die bei einer Reproduktion Moiremuster erzeugen, entsteht ein zusätzlich wirksamer Kopierschutz.



► *Relief und Kopierschutz*

Spezialraster

Satt über Rasterpunkte werden die Motive von Hochsicherheitsdokumenten durch speziell erzeugte, ein- und mehrfarbige Musterraster dargestellt.



► *Spezialraster einfarbig, vierfarbig, Spezialrasterkombination*

Digitale Wasserzeichen

Über das Sicherheitsmerkmal des digitalen Wasserzeichens kann einem Bild eine zusätzliche Information zugeordnet werden, die für das Auge unsichtbar bleibt und erst beim Scannen durch eine entsprechende Software erkennbar wird. Die insbesondere in Personalisierungsverfahren zusätzlich eingefügte individuelle Bildinformation schließt ein einfaches Austauschen von Bildern in ID-Dokumenten aus.

Sicherheit der Originaldaten

Besonderes Augenmerk gilt dem Schutz und der zuverlässigen Sicherung von Originaldaten. In der Bundesdruckerei verfügt das Datenverarbeitungsnetz, in dem die Muster erzeugt und verarbeitet werden, über einen eigenen Server, der abgekoppelt vom Unternehmensnetz im Hochsicherheitsbereich des Trustcenters betrieben wird. Die Lagerung archivierter Daten sowie die Tagessicherungen erfolgten innerhalb eines Hochsicherheitsrings in einem separaten Brandabschnitt. Selbstverständlich wird die Datensicherheit regelmäßig auditiert.

Komplexe optisch variable Merkmale

Für alle deutschen ID-Dokumente hat die Bundesdruckerei ein individualisiertes Volumenhologramm (Identigram®) in den Herstellungsprozess integriert. Auf diese Weise sind wesentliche Teile der optischen Personalisierung, wie das holografische Porträt (HSP Holographic Shadow Picture), der 3D-Bundesadler, die kinematische Bewegungsstruktur, die Makro- und Mikroschriften, die holographische Wiedergabe der maschinenlesbaren Zeilen und das maschinenlesbare Merkmal auch als Volumenhologramm verfügbar.



► Identigram® auf der Datenseite des deutschen Reisepasses und Personalausweises

Nummerierung

Jedes Dokument erhält eine eindeutige Nummer, wobei der entsprechende Nummernkreis bereits im Vorfeld eines Auftrags festgelegt und in der Regel alphanumerisch (zur Kennzeichnung unterschiedliche Serien) aufgesetzt wird. Über dieses Verfahren bleibt jedes Einzeldokument in der gesamten ID-Prozesskette identifizier- und verfolgbar und kann im Falle eines Diebstahls mit einer eindeutigen Kennung international gemeldet werden. Die Nummerierung von Blanko-Dokumenten bildet somit einen wesentlichen Bestandteil der Sicherheitslogistik.

Drucknummerierung

In den Hochdrucknummerierwerken der Bundesdruckerei können alle ID-Dokumente - auch in den verwendeten Farben - mit zusätzlichen numerischen Sicherheitsmerkmalen (z. B. IR unsichtbar/sichtbar, UV, magnetische Eigenschaften) ausgestattet werden. Ein normaler Strichbarcode ist ebenfalls möglich, wird in der Regel jedoch nur auf einer der Seiten aufgebracht.

Mechanische Perforation

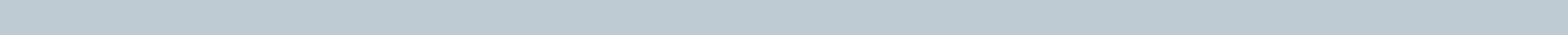
Die mechanische Perforation des Buchblocks (z. B. eines Reisepasses) erfolgt von der ersten bis zur letzten Seite des Dokuments, wobei die Durchmesser der Löcher mit aufsteigenden Seitenzahlen sinken.

Laserperforation

Weil die Ränder gelasierter Perforationslöcher teilweise erkennbare Schmauchspuren aufweisen, kann die Sicherheit des ID-Dokuments über dieses Verfahren nochmals gesteigert werden. Während einer Laserperforation ist zudem die Nummerierung der Vorderseite des Datenblattes möglich.

► Auszug aus den Referenzen

Pässe	<ul style="list-style-type: none"> Deutschland UK China Bosnien Albanien Rumänien Litauen
ID-Karte	<ul style="list-style-type: none"> Deutschland Litauen Rumänien foreigner ID
Führerscheine	<ul style="list-style-type: none"> Deutschland Island Portugal Litauen Ukraine
Visa	<ul style="list-style-type: none"> EU-Visum Deutschland
Weitere	<ul style="list-style-type: none"> Die Tachographkarte UK Die Signaturkarte am Beispiel des digitalen Dienstaussweises Die Trusted Traveller Card



► KONTAKT

Bundesdruckerei GmbH
Oranienstraße 91
10958 Berlin-Germany
Phone +49 (0) 30 - 25 98-0
Fax +49 (0) 30 - 25 98-22 05
E-Mail id@bdr.de
www.bundesdruckerei.de