BUNDESDRUCKEREI

ePASS POCKET GUIDE 2013

INHALT

EINLEITUNG

Wie der ePass die Mobilität der Zukunft prägen wird

Mit der Globalisierung hat sich die Art, wie Menschen reisen, stark verändert. Wer heute einen internationalen Flughafen betritt, trifft auf Geschäftsreisende aus der ganzen Welt. Man begegnet Touristen, unterwegs in weit entfernte Länder, die bis vor wenigen Jahrzehnten nur wenige Abenteurer besuchten. Manche der Flughafengäste sind auf dem Weg in eine neue, bessere Heimat, andere zu einem Meeting oder einem Forschungsaufenthalt. Nicht alle, die auf ihren Flug warten, halten sich an Recht und Gesetz: Illegale Einwanderung, Drogenhandel und Terrorismus sind zu weltweiten Phänomenen geworden, die die internationale Staatengemeinschaft vor große Herausforderungen stellen.

Moderne Staaten wollen ihren Bürgern dennoch sichere, unkomplizierte Mobilität ermöglichen. Dafür benötigen sie Reisedokumente, die aktuellsten Sicherheitsanforderungen gerecht werden. Das Ziel: Ausweise, die ihre Inhaber eindeutig identifizieren, den bestmöglichen Schutz vor Fälschungen und Manipulationen bieten und gleichzeitig ein komfortables Reiseerlebnis ermöglichen. Die Mobilität der Zukunft wird maßgeblich geprägt sein von Ausweisdokumenten wie dem ePass. Über seinen integrierten Chip ist er in eine komplexe Sicherheitsarchitektur eingebunden, die hohen Anforderungen und Standards gerecht wird.

Die Bundesdruckerei ist Vorreiter im Bereich elektronischer Reisedokumente. Bereits 2005 hat sie den weltweit ersten ePass vorgestellt. Seine innovative Technologie ist in Passprojekte mehrerer Staaten eingeflossen. Nicht nur die Bundesrepublik Deutschland, sondern zunehmend auch andere Nationen setzen heute auf das Know-how des Unternehmens in Sachen elektronischer Reisedokumente. Als Full-Service-Anbieter steht die Bundesdruckerei ihren Auftraggebern in allen Projektphasen zur Seite, von der Konzeption bis hin zur Verifikation der Ausweisdokumente. Sie ist der richtige Partner, wenn es darum geht, eine passende, qualitativ hochwertige Lösung für Ihren Bedarf zu finden. Die Bandbreite der technischen Möglichkeiten ist dabei nahezu unbegrenzt. Welche Anforderungen dabei zu beachten sind und welche Technologien zur Verfügung stehen: All das lesen Sie auf den folgenden Seiten.

KAPITEL 1
SICHERE REISEDOKUMENTE FÜR DAS 21. JAHRHUNDERT

Wie sich Reisepässe im Laufe der Zeit verändert haben – und welchen gestiegenen Anforderungen sie gerecht werden müssen

Wer von einem Land in ein anderes reist, muss sich ausweisen können. Dieses Prinzip kannten bereits die alten Römer, die ihre Abgesandten mit versiegelten Schriftrollen als Identitätsnachweis durch die Welt schickten. Ab dem Mittelalter wurden hoheitliche Ausweisdokumente für immer breitere Personenkreise zur Pflicht: In vielen europäischen Regionen mussten zunächst Soldaten, ab dem 16. Jahrhundert zunehmend auch Kaufleute Identitätspapiere mit sich führen. Diese erfüllten häufig zusätzlich die Funktion als Schutzbriefe eines Landesherren, die ihrem Inhaber freies Geleit in fremden Ländern sichern sollten. Noch heute trägt etwa der britische Pass ein entsprechendes Schutzersuchen. Pässe, die ihre Inhaber grundsätzlich zum internationalen, grenzüberschreitenden Reisen berechtigen, sind seit Beginn des 20. Jahrhunderts international üblich. 1920 gab der Völkerbund erste Richtlinien für solche Dokumente aus, die Vereinten Nationen und diverse internationale Gremien entwickeln sie seitdem kontinuierlich weiter. Waren bis zum Ende des 20. Jahrhunderts ausschließlich auf Papier basierende Pässe ohne Elektronik im Umlauf, so setzen sich heute moderne ePässe mit integriertem Chip immer mehr durch. Sie verfügen entweder über eine papierbasierte Datenseite oder ein entsprechendes Pendant aus Polycarbonat (PC).

Die Aufgaben von Pässen sind dabei überall auf der Welt gleich. Als Identitätsnachweis bestätigen sie gegenüber staatlich autorisierten Instanzen, dass die eingetragenen Personalien mit den Personendaten des Passinhabers übereinstimmen. Sie dokumentieren, dass dieser Staatsbürger einer bestimmten Nation ist – und ermöglichen es, über die Grenze des ausstellenden Staates ins Ausland und wieder zurückzureisen. Wer einen Reisepass besitzt, hat außerdem Anspruch auf den Schutz durch diplomatische Vertretungen des Ausstellerstaats. Fremden Staaten gegenüber garantiert das Dokument, dass das Herkunftsland den Inhaber des Dokuments wieder aufnimmt, sollte sein Aufenthaltstitel für das Gastland ablaufen oder seine Gültigkeit verlieren. Pässe sind damit eine wesentliche Voraussetzung dafür, dass grenzüberschreitende Mobilität in geregelten Bahnen ablaufen kann. Sie sind Türöffner für Reisende auf der ganzen Welt und geben Bürgern wie staatlichen Stellen Sicherheit.

Der Wunsch der Menschen nach weltweiter Mobilität hat zugenommen. In den vergangenen Jahren sind deshalb auch die Anforderungen an Reisedokumente deutlich gestiegen. Die wohlhabenden Industrienationen und die aufstrebenden Ökonomien in den Schwellenländern sind heute wirtschaftlich stärker verflochten denn je. Eine Vielzahl von Unternehmen hat sich international aufgestellt und Niederlassungen rund um den Globus eröffnet. Fach- und Führungskräfte aus diversen Ländern treffen sich heute auf einer Konferenz in einer asiatischen Metropole, reisen morgen weiter zu ihren Kunden in Übersee und am Tag darauf zurück in ihre Heimatländer. Bevölkerungswissenschaftler stellen zudem fest, dass immer häufiger auch Menschen aus Industrienationen auf Dauer in ein anderes Land auswandern.

Internationale Flughäfen haben sich somit auf der ganzen Welt zu hoch frequentierten Drehkreuzen für Mobilität entwickelt. Im Schnitt steigt die Zahl der Passagiere, die internationale Flüge buchen, laut der internationalen Flughafenvereinigung Airport Council International (ACI) jährlich im Schnitt um fast sechs Prozent (Quelle: Pressemitteilung des ACI vom 5. Juni 2012). Dank des technischen Fortschritts und der gesunkenen Preise für die Personenbeförderung sind weite Reisen längst kein Privileg von Wohlhabenden mehr: Einen Urlaub in Thailand, einen Wochenendtrip in eine pulsierende Großstadt leisten sich in vielen Ländern der Welt heute auch Normalverdiener. Da gerade in aufstrebenden Staaten

wie China oder Indien die Mittelschicht weiter wächst, wird sich dieser Trend in Zukunft noch verstärken.

Allerdings werden auch die Schattenseiten der beschleunigten Globalisierung zunehmend sichtbar. Auf der Suche nach einem besseren Leben verlassen verstärkt Flüchtlinge ihre Heimatländer, häufig angelockt von den Versprechungen zweifelhafter Schlepperbanden. Zudem wächst die Furcht vor terroristischen Anschlägen, weil auch gewaltbereite Fanatiker sich die Möglichkeiten moderner internationaler Mobilität zunutze machen. Persönliche Daten sind zudem zur Handelsware geworden, mit der sich kriminelle Geschäftemacher hohe Gewinne sichern wollen: Gerade in ärmeren Ländern versuchen spezialisierte Banden immer noch, Ausweispapiere zu fälschen oder zu manipulieren, um so die Einreise in wohlhabendere Länder zu ermöglichen. Gleichzeitig ist der Identitätsdiebstahl im Netz, bei dem sensible Daten von Bürgern missbräuchlich eingesetzt werden, weltweit zu einem ernsthaften Problem geworden. Vor diesem Hintergrund wird klar, warum das Sicherheitsbedürfnis in zahlreichen Staaten in der jüngsten Vergangenheit deutlich gewachsen ist. Hoheitliche Stellen ebenso wie Bürger und Wirtschaft wünschen sich Abwicklungsprozesse im internationalen Reiseverkehr, die sicher und gleichzeitig für alle Beteiligten möglichst einfach zu handhaben sind.

Umso wichtiger sind Reisedokumente, die mit den neuen Anforderungen Schritt halten. Sie müssen so konzipiert sein, dass das Grenzpersonal Fälschungen schnell und sicher erkennt, im besten Fall bereits mit bloßem Auge. Selbst wenn sich in Stoßzeiten auf Flughäfen, auf Bahnhöfen oder an Landesgrenzen eine Vielzahl von Reisenden drängt, ist eine komfortable Abfertigung zu gewährleisten, ohne dass die Sicherheit gefährdet wird. Viele Bürger und Regierungen pochen zudem auf einen möglichst umfassenden Datenschutz für die auf dem Chip der Dokumente gespeicherten persönlichen Daten. Damit sie nicht missbräuchlich verwendet werden können, darf stets nur ein eng begrenzter Kreis hoheitlich autorisierter Stellen darauf Zugriff haben. Außerdem sollten nur diejenigen Datenkategorien auf dem Chip geprüft werden können, die zur zuverlässigen Authentifizierung einer Person tatsächlich nötig sind.

Noch bis vor wenigen Jahren standen ausschließlich papierbasierte Ausweisdokumente zur Verfügung, um diesen Herausforderungen zu begegnen. Die klassischen Sicherheitsmerkmale, die dabei zum Einsatz kommen, haben Anbieter wie die Bundesdruckerei im Laufe der Jahre immer weiter perfektioniert. Mit speziellen Fasern, Mustern oder Farben (vgl. Kapitel 3) ist es so gelungen, für Fälscher kaum überwindbare Hürden zu schaffen. Die holografischen Sicherheitsmerkmale etwa, die die Bundesdruckerei über das sogenannte Identigram® bereits seit 2001 in den deutschen Reisepass und den deutschen Personalausweis einbringt, haben international neue Standards gesetzt. Solche optischen Merkmale kombiniert die Bundesdruckerei mit den klassischen, aber auch mit maschinenlesbaren Sicherheitsfunktionen individuell für jedes Passprojekt. Vor allem sogenannte Level-1-Merkmale, die sich mit bloßem Auge erkennen lassen, liegen dabei heute im Trend: Sie ermöglichen dem Personal an der Grenzkontrolle, ohne Hilfsmittel festzustellen, ob ein Pass gefälscht oder echt ist. So lässt sich auch an Grenzstationen, die nicht über eine hochtechnologische Ausstattung verfügen, ein hohes Maß an Sicherheit gewährleisten.

Seit einigen Jahren haben die ausstellenden Staaten außerdem die Wahl zwischen Pässen mit papierbasierter Datenseite und solchen mit einer Datenseite aus robustem Polycarbonat. Klassische und maschinenlesbare Sicherheitsmerkmale können in beiden Varianten eingesetzt werden. Die Kombination und Auswahl dieser Merkmale sind für jedes Passprojekt individuell. Welche Passvariante sich am besten für ein Land eignet, muss deshalb stets im Einzelfall entschieden werden. In der Europäischen Union zum Beispiel hat bereits über die Hälfte der Mitgliedsstaaten die PC-Passvariante gewählt. Während Pässe mit Papierdatenseiten per Inkjet-Verfahren personalisiert werden, graviert man die individuellen Daten in PC-Pässe mit einem Laser in den Kunststoff. Das garantiert ein hohes Maß an Fälschungssicherheit, weil kaum ein potenzieller Fälscher Zugang zu entsprechenden Lasern hat. Entscheidend für die individuelle Wahl der Passvariante ist, wie der ausstellende Staat mit den Vorgaben der ICAO (vgl. Kapitel 2) umgeht und wie viel er in sein Passprojekt investieren will. Weiterhin muss berücksichtigt werden, ob er eine zentrale oder eine dezentrale Personalisierung bevorzugt und wie die Pässe in bestehende Sicherheitsarchitekturen eingebunden werden sollen.

Die wohl wichtigste Entwicklung in der jüngsten Passgeschichte ist jedoch der elektronische Reisepass (ePass). Dank seines Chips sorgt er für ein noch höheres Sicherheitsniveau im Vergleich zu rein analogen Ausweisdokumenten. Beide Passvarianten können mit einem

integrierten Chip ausgestattet werden: Beim Inkjet-ePass mit papierbasierter Datenseite wird der Chip im eigens von der Bundesdruckerei entwickeltem Flexcover integriert. Entscheiden die Auftraggeber sich für einen PC-Pass, wird der Chip in der PC-Datenseite platziert. Gespeichert sind darauf neben den Personendaten, die auch optisch personalisiert sind, meist zusätzliche biometrische Informationen, wie etwa das Gesichtsbild und Fingerabdrücke des Passinhabers. Dass es sich um einen ePass handelt, erkennt man am von der ICAO vorgegebenen Symbol auf dem Cover.

Da die Daten sowohl optisch als auch in elektronischer Form auf dem Pass vorhanden sind, sind Manipulationen einfacher festzustellen. Vor allem erleichtern ePässe dem Grenzpersonal die Kontrolle der Dokumente: Mithilfe spezieller Lesegeräte können die staatlich autorisierten Kontrolleure die biometrischen Daten auf dem Chip sowohl mit den Daten auf dem Dokument als auch mit denen der physisch anwesenden Person abgleichen. Dadurch wird es zum Beispiel einfacher, Personen zu identifizieren, mit deren Physiognomie die Kontrolleure nicht vertraut sind. Umfangreiche Sicherheitsmechanismen sorgen dafür, dass Manipulationen oder Totalfälschungen des Chips nahezu unmöglich sind und nur befugte Personen Zugriff auf die darauf gespeicherten Daten haben. Die Technologie ermöglicht zudem automatische Passkontrollen, was die Abfertigung für Reisende und Grenzpersonal zusätzlich vereinfacht. Länder wie Malaysia nutzen sogenannte eGates bereits seit einigen Jahren, in Europa steht die Einführung noch am Anfang.

Der Siegeszug der elektronischen Reisepässe ist längst nicht mehr aufzuhalten. Das gewachsene Sicherheitsbedürfnis gerade der westlichen Länder nach dem 11. September 2001 war ein Auslöser für die Einführung von ePässen. Die Europäische Union verpflichtete ihre Mitgliedsländer bereits 2004 dazu, elektronische Reisepässe mit biometrischen Merkmalen einzuführen. Heute sind weltweit bereits fast 340 Millionen ePässe in Umlauf. Derzeit knapp 100 Staaten statten ihre Bürger mit den elektronischen Reisedokumenten aus. Über 60 Staaten speichern dabei biometrische Daten der Inhaber auf dem Chip des Passes. Ende des Jahres 2016, schätzt die Unternehmensberatung Smithers Pira, werden 90 Prozent aller ausgegebenen Pässe mit Chips versehen sein (vgl. Studie „The Future of Personal Identification – market and technology forecasts to 2016“, Smithers Pira 2010, S. 67).

Ob es um ePässe oder herkömmliche Reisepässe geht, reine Papierdokumente oder Pässe mit einer PC-Seite: Die Bundesdruckerei bietet ihren Kunden maßgeschneiderte Lösungen für ihren Bedarf an – und begleitet sie von Anfang an, schon bei der Entwicklung der Spezifikationen für ein Passprojekt. Auch heute noch liefert das Unternehmen klassische, rein analoge Pässe aus, etwa für Staaten wie Litauen und Rumänien. Ihre Kompetenz in Sachen elektronischer Reisepass hat die Bundesdruckerei zunächst mit der ersten und zweiten Generation des deutschen ePass unter Beweis gestellt. Beide Male hat das Unternehmen die Einführung maßgeblich vorbereitet und mit einem umfangreichen Servicepaket unterstützt. Für die dritte Generation des ePass soll die bewährte Partnerschaft mit dem deutschen Bundesinnenministerium fortgesetzt werden. Innerhalb Europas stattet die Bundesdruckerei außerdem Länder wie Bosnien, Luxemburg und Zypern mit ePass-Lösungen aus. Alle drei Länder beziehen zudem nicht allein die Ausweisdokumente von der Bundesdruckerei, sondern jeweils auch maßgeschneiderte Lösungen zur Personalisierung.

Längst vertrauen auch Staaten außerhalb Europas auf die Unterstützung aus Berlin. Bis 2014 soll mithilfe des Unternehmens zum Beispiel rund eine Million ePässe für die Vereinigten Arabischen Emirate (VAE) hergestellt werden. Zusammen mit dem Innenministerium der Vereinigten Arabischen Emirate betreibt die Bundesdruckerei dafür seit 2011 ein Joint Venture in Abu Dhabi. Bereits seit 2007 ist die Bundesdruckerei auf dem südamerikanischen Markt aktiv: Venezuela, das erste lateinamerikanische Land, das ePässe eingeführt hat, bezieht Polycarbonat-Passkarten mit integriertem Chip aus Berlin. Vor Ort werden sie mithilfe eines ebenfalls von der Bundesdruckerei gelieferten Personalisierungssystems mit den persönlichen Daten der Passinhaber versehen. Solchen Hightech-Lösungen gehört die Zukunft: Sie sind für die Herausforderungen einer immer komplexer werdenden Welt am besten gerüstet.

KAPITEL 2
STANDARDS ALS GARANT FÜR REIBUNGSLOSE MOBILITÄT

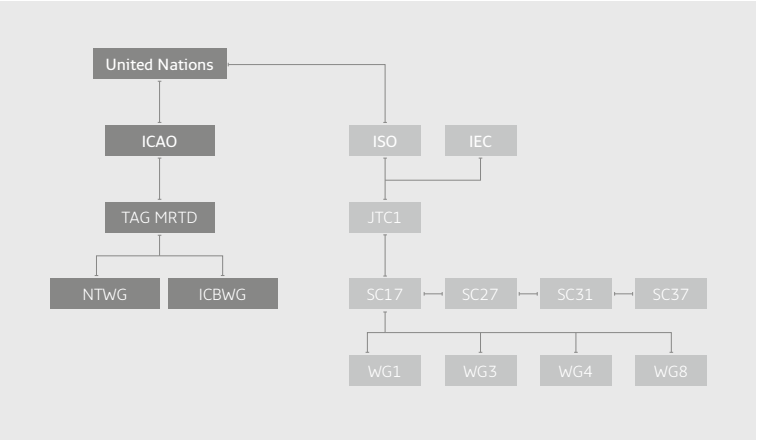
Welche Normen ein moderner Reisepass erfüllen muss – und wer für die Vorgaben verantwortlich ist

Einheitliche Dokumentenstandards sorgen für mehr Sicherheit und Komfort auf Reisen. Sie erleichtern es den Grenzbeamten, die Gültigkeit der Ausweisdokumente schnell und zuverlässig zu prüfen. Zum Teil erlauben sie es Reisenden sogar, vollautomatisierte Kontrollen zu passieren. Die Vorschriften für Reisedokumente legen auf internationaler Ebene Experten fest, etwa Gremien der Internationalen Zivilluftfahrt-Organisation (International Civil Aviation Organization, ICAO), der Europäischen Union und der Internationalen Organisation für Normung (International Organization for Standardization, ISO). Insbesondere für hoheitliche Identitätsdokumente gibt die ICAO, eine Sonderorganisation der Vereinten Nationen, die grundsätzlichen Leitlinien vor. Sie ist 1944 von 190 Mitgliedsländern gegründet worden, um durch multilaterale Regelungen die Luftfahrt zu unterstützen und zu mehr Sicherheit beizutragen. Im „Chicagoer Abkommen“ bekam die ICAO noch im gleichen Jahr das Mandat, auch internationale Standards und Spezifikationen für Reisedokumente zu definieren. Die Bundesdruckerei ist in den unterschiedlichen Gremien der ICAO vertreten und kann so ihre Erfahrung in der Herstellung von Dokumenten in die Entwicklung von bestehenden und neuen Standards einbringen.

An der Standardisierung beteiligte Organisationen

Gremien und ihnen untergeordnete Arbeitsgruppen, die bei der Entwicklung von Dokumentenstandards mitwirken:

ABBILDUNG 1: ORGANISATIONEN ZUR STANDARDISIERUNG VON REISEPÄSSEN



> **International Civil Aviation Organization (ICAO), Montréal, Kanada**
Internationale Organisation zur Förderung der zivilen Luftfahrt, legt Standards für internationale Reisedokumente wie etwa für Reisepässe und Aufenthaltstitel fest.

> **Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD)**
Entwirft und verabschiedet Spezifikationen für maschinenlesbare Reisedokumente, die von der ICAO in Dokument 9303 veröffentlicht werden. Zu den Mitgliedern zählen unter anderem Vertreter des Airports Council International (ACI), der International Air Transport Association (IATA), der Internationalen kriminalpolizeilichen Organisation (INTERPOL) und der ISO/IEC.

> **New Technologies Working Group (NTWG)**
Entwickelt die von der TAG/MRTD beauftragten Spezifikationen und legt dabei fest, welche neuen Technologien sich für den Einsatz bei Identitätsdokumenten eignen.

> **Implementation and Capacity Building Working Group (ICBWG)**
Unterstützt die Mitgliedsländer der ICAO bei der technischen Umsetzung der für Reisepässe relevanten Standards und Spezifikationen.

> **International Organization for Standardization (ISO), Genf, Schweiz**
Weltweit führende Organisation zur Entwicklung und Veröffentlichung von Standards, in der sich 162 nationale Standardisierungsorganisationen zusammengeschlossen haben. Versteht sich als Brücke zwischen öffentlichem und privatem Sektor und setzt Vorgaben von Organisationen wie der ICAO in konkrete technische Normen um.

> **International Electrotechnical Commission (IEC), Genf, Schweiz**
Weltweit führende Organisation zur Entwicklung und Veröffentlichung von Standards speziell für die Elektrotechnologie.

> **ISO/IEC Joint Technical Committee 1 (JTC 1)**
Gemeinsames Gremium von ISO und IEC zur Entwicklung von Normen für die Informationstechnik.

> **Sub-Committee 17 (SC17)**
Arbeitet für das Gremium ISO/IEC JTC 1 unter anderem an der Normierung von Reisedokumenten und von Anwendungen zur persönlichen Identifikation.

> **ISO Working Group 1 (WG1)**
Entwickelt Prüfmethoden zur Stabilität und Sicherheit von Identifikationskarten und -dokumenten, darunter auch Reisepässe.

> **ISO Working Group 3 (WG3)**
Entwickelt im Auftrag der ICAO technische Festlegungen für maschinenlesbare Reisedokumente, die in die Standardserie ICAO 9303 Eingang finden. Dabei kooperiert sie mit den Working Groups WG1, WG4 und WG8.

> **ISO Working Group 4 (WG4)**
Normt die logische Datenstruktur von Chips und die Krypto-Verfahren, mittels derer Daten gesichert ausgetauscht werden.

> **ISO Working Group 8 (WG8)**
Entwickelt Standards für den kontaktlosen Datenaustausch an Schnittstellen zu Chips, maschinenlesbaren Reisedokumenten und mobilen Endgeräten.

> **Sub-Committee 27 (SC27)**
Entwickelt Standards für IT-Sicherheitstechniken, zum Beispiel für Krypto-Verfahren und -Algorithmen.

> **Sub-Committee 31 (SC31)**
Entwickelt Standards für maschinenlesbare Zeichen und Barcodes sowie für ihre Qualitätsprüfungen.

> **Sub-Committee 37 (SC37)**
Entwickelt Biometrie-Standards für Identitätsdokumente und andere Objekte zur Identitätskontrolle, die zum Beispiel den Zutritt zu Gebäuden regeln.

> **Comité Européen de Normalisation (CEN), Brüssel, Belgien**
Europäisches Pendant zur ISO.

> **CEN/Technical Committee 224 (TC 224)**
Europäisches Pendant zum SC17. Entwickelt unter anderem EU-weite Normen für elektronische Reisedokumente sowie die damit verknüpften Systeme und Anwendungen.

> **Article-6-Group der Europäischen Union**
Legt fest, welche Anforderungen Identitätsdokumente der EU-Mitgliedsländer erfüllen müssen.

STANDARDS MODERNER REISEDOKUMENTE

International gültige Reisedokumente sind, wie in Kapitel 1 erläutert, heute nicht mehr als reine Sichtausweise konzipiert, sondern vielfach bereits mit einem integrierten Chip ausgestattet. Laut ICAO-Vorgabe haben sie das Format ID3 (125×88 Millimeter) und enthalten eine maschinenlesbare Zone (Machine Readable Zone, MRZ). Die Spezifikationen dafür sind im ICAO-Dokument 9303 festgehalten. Aus welchen Materialien Reisepässe angefertigt werden, können die ausgebenden Staaten selbst entscheiden. Sie müssen allerdings sicherstellen, dass die Pässe bei normalem Gebrauch die Gültigkeitsdauer von fünf bis zehn Jahren schadlos überstehen. Dazu müssen die Pässe laut ICAO bestimmte physikalische Eigen-

schaften aufweisen: Sie sollten starken Temperaturunterschieden standhalten sowie gegenüber Chemikalien und Feuchtigkeit resistent sein. Zudem dürfen die Materialien bei intensivem Lichteinfall nicht porös werden oder die Funktionalität anderer Komponenten des Reisepasses – wie etwa den Chip – negativ beeinflussen. Um Brüche zu vermeiden, ist im ICAO-Dokument 9303 die Verwendung biegsamer Materialien vorgeschrieben. Mittels Stress-Tests lässt sich überprüfen, ob die physikalischen Anforderungen der ICAO erfüllt werden. Entsprechende Versuchsanordnungen hat die International Organization for Standardization (ISO) entwickelt. Die Durchführung dieser Tests ist für die Mitgliedsstaaten der ICAO allerdings nicht verbindlich.

Aktuell wird an einer Neuauflage des Dokuments 9303 gearbeitet. Die derzeit gültige Fassung dieses Standards umfasst die drei Teile Reisepässe (Teil 1), Visa (Teil 2) und sonstige amtliche Reisedokumente (Teil 3). Im Einzelnen fordert die ICAO zurzeit Folgendes:

Standards, die für alle Reisepässe gelten:

> **Maschinenlesbarkeit (Dok. 9303 Part 1, Volume 1 – Richtlinie für ICAO-konforme maschinenlesbare Reisepässe)**
Die Maschinenlesbare Zone ICAO-konformer Reisepässe enthält in der Regel zwei bis drei Zeilen mit Informationen. Aufgedruckt sind sie in einem Standardformat und der Standardschrift OCR-B, die Ende der 1960er-Jahre speziell zur Erleichterung der maschinellen Zeichenerkennung entwickelt wurde. Angegeben sind hier Name, Geburtsdatum und weitere Daten des Dokumenteninhabers. Prüfziffern ermöglichen eine Kontrolle des korrekten Einlesens der Daten mittels optischer Prüfgeräte. Grenzbeamte und andere berechtigte Stellen erfassen die Daten der maschinenlesbaren Zone mittels optischer Lesegeräte, wie sie auch die Bundesdruckerei anbietet, und übermitteln sie direkt an ein hoheitliches IT-System. Das steigert die Effizienz bei der Dokumentenprüfung und verhindert, dass der Kontrolleur versehentlich per Hand falsche Daten ins System eingibt. Damit das Dokument im Sinne der ICAO als maschinenlesbar gilt, muss das zusätzlich vorgeschriebene Foto des Inhabers bestimmte Abmessungen haben und auf besondere Art angeordnet sein. Bis 2015, fordert die ICAO, sollen die Mitgliedsländer alle konventionellen Reisepässe durch ihre moderneren, maschinenlesbaren Pendants ersetzen.

Standards, die für elektronische Reisepässe gelten:

> **Biometrische Identifizierung (Dok. 9303 Part 1, Volume 2 – Richtlinie für ICAO-konforme elektronische Reisepässe)**
Die ICAO sieht drei biometrische Identifizierungsmöglichkeiten vor. Zum einen die Gesichtserkennung, die bereits verbindlich vorgeschrieben ist, zum anderen Fingerabdrücke und Iriserkennung als Optionen. Sind solche Merkmale einer Person auf dem Chip des Ausweisdokuments gespeichert, kann deren Identität bei jeder Ein- und Ausreise bestätigt werden. Dafür vergleichen Grenzkontrolleure die Merkmale mit dem Bild auf dem Dokument beziehungsweise mit den Daten auf dem Chip. Bei Bedarf beziehen sie zur Kontrolle auch Informationen aus einer Datenbank mit ein. Kryptografische Verfahren stellen sicher, dass die Daten echt und unverfälscht auf dem Chip vorliegen und lediglich von berechtigten Stellen ausgelesen werden können.

> **Konzeption des Sicherheits-Chips (Dok. 9303 Part 1, Volume 2 – Richtlinie für ICAO-konforme elektronische Reisepässe)**
Für den internationalen Reiseverkehr zugelassen sind nur kontaktlose Chips. Damit sie überall auf der Welt zuverlässig funktionieren, hat die ICAO eine standardisierte Datenstruktur und bestimmte Sicherheitsprotokolle definiert. Sie schützen vor missbräuchlichen Zugriffen und korrespondieren flexibel mit unterschiedlichen IT-Strukturen. In Kapitel 4 sind diese Vorgaben detailliert erläutert.

Trends bei der fortschreitenden Standardisierung von Reisedokumenten

Standardisierungsorganisationen arbeiten daran, die auf dem Chip gespeicherten Daten noch besser vor unbefugtem Zugriff zu schützen. Dazu sollten alle elektronischen Pässe, die sensible biometrische Daten wie den Fingerabdruck speichern, künftig über ein als Extended Access Control (EAC) bezeichnetes Zugriffsprotokoll verfügen. Eine Erweiterung dieses Sicherheitsprotokolls ist das sogenannte Supplemental Access Control (SAC), das ab 2014 alle auszugebenden elektronischen Pässe enthalten sollten. Es schützt die auf dem Chip gespeicherten Daten noch stärker vor unberechtigtem Zugriff. Wie die Sicherheitsprotokolle funktionieren, wird in Kapitel 4 beschrieben.

Ziel der ICAO ist es, dass auch vorläufige Reisedokumente mit kurzer Gültigkeitsdauer besser abgesichert werden. Die Vorgaben für entsprechende Sicherheitstechniken werden derzeit erarbeitet. Dabei wird berücksichtigt, dass aus Kostengründen nicht alle beim Reisepass angewendeten Sicherheitstechniken auf die vorläufigen Dokumente übertragen werden können. Um zu verhindern, dass Betrüger mit einer falschen Identität einen Reisepass beantragen, arbeitet die ICAO zudem an der Absicherung von Dokumenten und Systemen, die im Zusammenhang mit dem Reisepass von Bedeutung sind. Dazu zählen etwa die Verfahren zur Erstellung von Geburtsurkunden und Melderegisterauszüge. Die Ergebnisse der ICAO werden in einem Technical Report mit entsprechenden Empfehlungen zusammengefasst. Ob Staaten die Vorschläge der Experten für hoheitliche Dokumente anwenden, bleibt ihnen freigestellt. Um Manipulationen vorzubeugen und reibungslose Mobilität zu gewährleisten, ist die Einhaltung der ICAO-Standards aber in jedem Fall empfehlenswert.

KAPITEL 3
MERKMALE SICHERER DOKUMENTE

Warum es so wichtig ist, welche Merkmale ein Pass beinhaltet – und welche Trends sich abzeichnen

Eine der wichtigsten Anforderungen an einen Reisepass ist, dass er fälschungssicher ist. Das gilt sowohl für herkömmliche analoge Dokumente als auch für den neuen ePass. Der technologische Fortschritt der vergangenen Jahrzehnte hat zahlreiche neue Möglichkeiten geschaffen, Sicherheitsdokumente noch besser vor unbefugten Zugriffen und Manipulationen zu schützen.

Die Vielzahl der Merkmale wird unterschieden in Substratmerkmale, Farben, drucktechnische Anwendungsformen, haptische und mechanische Anwendungsformen sowie Folien und Overlays. Die unterschiedlichen Merkmale ergänzen sich gegenseitig und machen die Reisepässe so noch sicherer. Dank eines integrierten Chips verfügt der ePass zusätzlich über elektronische Sicherheitsmerkmale, die in Kapitel 4 erläutert werden.

Polycarbonat- oder Inkjet-Pass

Welche Sicherheitsmerkmale ein Land für seinen Pass genau wählt, hängt nicht nur davon ab, welche ICAO-Vorgaben es erfüllen will oder ob die Pässe zentral oder dezentral personalisiert werden, sondern auch von der gewählten Passvariante. Einige Sicherheitsmerkmale eignen sich nur für die papierbasierte Variante, den Inkjet-Pass, andere nur für den PC-Pass mit einer Datenseite aus Polycarbonat (vgl. Kapitel 1). In beiden Passvarianten werden sowohl klassische als auch moderne Hightech-Sicherheitsmerkmale eingesetzt.

Die Bundesdruckerei unterstützt ihre Auftraggeber dabei, die optimale Lösung für die jeweilige Aufgabenstellung zu finden. Aus diesem Grund sind auch nicht alle möglichen Sicherheitsmerkmale in dieser Publikation erläutert: Dokumentenschutz ist ein sensibles Thema, besonders innovative Lösungen erörtern die Experten der Bundesdruckerei im direkten Dialog.

Je komplexer, desto sicherer: das Prüfniveau

Um die Echtheit von Reisepässen feststellen zu können, müssen Grenzbeamte in der Lage sein, eingebrachte Sicherheitsmerkmale zu erkennen und zu überprüfen. Je komplexer die Merkmale sind, desto höher ist das Prüfniveau. Die Experten der Bundesdruckerei unterscheiden drei Level.

> Um die Merkmale von **Level 1** zu prüfen, reichen einfache Kenntnisse der Effekte aus. Sie sind mit bloßem Auge und ohne Hilfsmittel zu erkennen und kommen daher immer häufiger zum Einsatz. (siehe unten: Im Trend: leicht zu prüfende Merkmale)
> **Level 2** wird noch einmal unterteilt in **Level 2a** und **2b**. Merkmale von **Level 2a** sind mit einfachen Hilfsmitteln wie Lupe, UV-Lampe oder Filter zu erkennen. Für **Level 2b** benötigt der Prüfer spezielle Kenntnisse und Hilfsmittel, wie zum Beispiel Infrarotkameras, Verifikationsgeräte oder Laser.
> Detaillierte Kenntnisse sind für die Sicherheitsmerkmale von **Level 3** erforderlich. Diese können Prüfer nur mit spezieller Laborausstattung oder Sensoren wie einem Mikroskop, einem Spektrometer oder einem Röntgengerät erkennen und prüfen. (siehe Tabelle: „Funktion und Niveau der Sicherheitsmerkmale auf einen Blick“)

Funktion und Einsatz einzelner Sicherheitsmerkmale

Substrat

Das Trägermaterial von Pässen und ePässen, das sogenannte **Substrat,** besteht aus **Sicherheitspapier,** die Datenseite des PC-Passes aus **Polycarbonat.** Polycarbonat weist gute optische Eigenschaften sowie verarbeitungstechnische Vorteile auf. So ist es z. B. nahezu unzerbrechlich und hitzebeständig. Für Pässe, die eine lange Lebensdauer aufweisen und auf Reisen strapaziert werden, ist dieses Material daher hervorragend geeignet.

ABBILDUNG 2: POLYCARBONAT

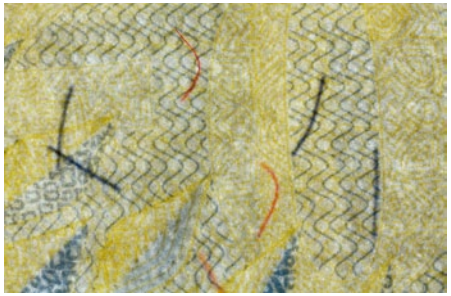
In das Sicherheitspapier der papierbasierten Seiten können verschiedene Stoffe integriert werden, zum Beispiel chemische Reagenzien, Fasern oder Sicherheitsfäden. Ein weiteres Sicherheitsmerkmal, das **Wasserzeichen,** entsteht durch Verschiebungen von Fasern im Papier, sodass einige Stellen optisch dichter sind, andere dünner. Im Durchlicht kann der Betrachter das Motiv des Wasserzeichens erkennen. Im Reisepass von Bosnien-Herzegowina sieht man zum Beispiel das Staatswappen und die Bezeichnung „BiH“ auf beiden Seiten der Datenseite. Wasserzeichen schützen ein Dokument vor Kopie und Totalfälschung.

ABBILDUNG 3: WASSERZEICHEN

Chemische Reagenzien hingegen ermöglichen es, Manipulationsversuche am Dokument sichtbar zu machen. Sie können in Druckfarben oder direkt in das Substrat eingebracht werden. Kommen sie mit Säuren, Laugen oder Lösungsmitteln in Kontakt, verändern sich die Farben im Dokument oder bluten aus. Wasserzeichen und chemische Reagenzien sind Sicherheitsmerkmale, die nur für Papier geeignet sind.

Für die Veredlung beider Trägermaterialien – Papier und PC – werden weitere Sicherheitsmaterialien zugeführt. Ein Beispiel hierfür sind **Melierfasern.** Die Kunststoff-Fasern werden bei der Herstellung unter das Substrat gemischt und befinden sich so an zufälligen Stellen im Papier. In Polycarbonat-Seiten kommen sie nur selten zum Einsatz, da nur wenige Firmen wie z. B. die Bundesdruckerei diese Technologie beherrschen. Die verschiedenfarbigen Fasern sind 0,3 Millimeter dick und mit bloßem Auge oder unter UV-Licht zu sehen. Beim zypriotischen Reisepass zum Beispiel sind die Fasern gleichmäßig im Papier verteilt. Sie fluoreszieren unter UV-Licht in Rot und Blau.

ABBILDUNG 4: MELIERFASERN



Ähnliches gilt für **Sicherheitsfäden:** Ein Sicherheitsfaden aus Metall oder Kunststoff kann innen oder außen auf dem Trägermaterial, Papier oder Polycarbonat, angebracht werden, durchgängig verlaufen oder fensterartig angeordnet sein, in diesem Fall liegt er teilweise frei. Sicherheitsfäden können gefärbt, fluoreszierend, mit Mikrotext bedruckt, holografisch und maschinell prüfbar sein. Ebenso wie Melierfasern schützen auch Sicherheitsfäden die Ausweisdokumente vor Reproduktionsversuchen und Totalfälschungen. Es ist nahezu unmöglich für Fälscher, sie nachzubilden oder sich gleichwertige Materialien zu beschaffen.

ABBILDUNG 5: SICHERHEITSFADEN

Ob ein Pass gefälscht ist, können Grenzbeamte auch daran erkennen, wie die **Heftfäden** zusammengesetzt sind, die die Seiten des Passbuches zusammenhalten. Die Fäden bestehen aus mehreren Kunststoff- oder Baumwolladern, die zum Teil auch unter UV-Licht fluoreszieren können. Der gelb-grün-weiße Heftfaden des zypriotischen Reisepasses zum Beispiel leuchtet unter UV-Licht grün. Die Breite der Nähstiche kann ein weiteres Indiz für eine Totalfälschung liefern.

ABBILDUNG 6: HEFTFADEN

Farben

Der Einsatz besonderer Farben sorgt für charakteristische Effekte und hohe Fälschungssicherheit von Reisepässen. Farben lassen sich nach dem Level ihrer Überprüfbarkeit unterscheiden.

Level-1-Effektfarben

Level-1-Effektfarben sind irisierende, optisch variable sowie thermochromatische Farben. **Irisierende Farben** enthalten winzige Glimmerplättchen, die als Spiegel fungieren und das einfallende Licht je

nach Betrachtungswinkel unterschiedlich zurückwerfen. Die Farbe schimmert perlmuttartig.

ABBILDUNG 7: IRISIERENDE FARBEN

In **optisch variable Farben** (engl. Optically Variable Ink, **OVI**) sind spezielle Pigmente eingebettet, die eine besondere Struktur aufweisen. Dadurch ändert sich die Farbe je nach Betrachtungswinkel oder Lichteinfall. Das Kürzel UAE im Vorsatz des Passes der Vereinigten Arabischen Emirate ändert so zum Beispiel seine Farbe von Magenta zu Grün.

ABBILDUNG 8: OPTISCH VARIABLE FARBEN

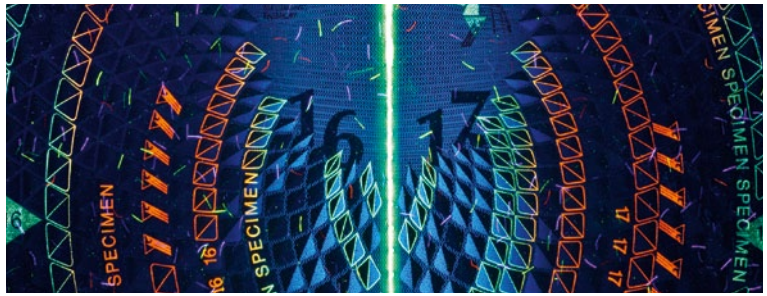
Thermochromatische Farben verändern sich, wenn man sie erwärmt, zum Beispiel indem man sie in den Händen hält. Wenn die Farbe eine bestimmte Temperatur erreicht hat, wird sie transparent und eine darunterliegende Information wird sichtbar oder ein anderer Farbton entsteht. Dieser Effekt ist reversibel und kann beliebig oft wiederholt werden.

Alle Level-1-Farben schützen den Pass vor Reproduktionsversuchen und sind mit bloßem Auge oder einfachen Hilfsmitteln zu erkennen.

ABBILDUNG 9: THERMOCHROMATISCHE FARBEN

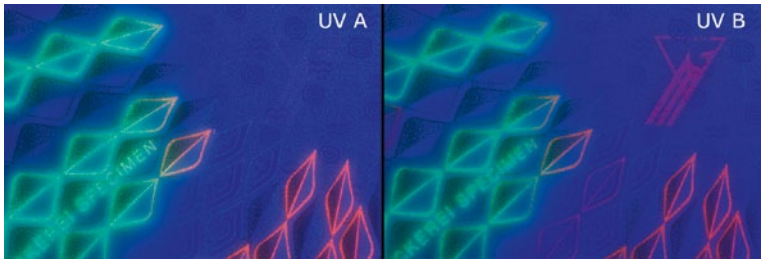
Level-2- und -3-Effektfarben:
Farben für ein noch höheres Prüfniveau
Weniger leicht zu überprüfen sind Level-2-Effektfarben. Um sie zu kontrollieren, benötigt man Hilfsmittel wie Infrarot- oder UV-Lichtquellen. Zu den Level-2-Effektfarben gehören zum Beispiel UV-Fluoreszenz-, Bi-Fluoreszenz-, Up-Conversion-, UV-Absorber-, UV-Phosphoreszenz-, IR-Effekt-, fotochrome, metamerische und magnetische Farben. **UV-fluoreszierende Farben** enthalten Pigmente, die unter einer UV-Lampe sichtbar werden. Die Körperfarbe der UV-fluoreszierenden Farbe kann sichtbar oder unsichtbar sein. Fluoreszierende Farben können auch im Irisdruckverfahren aufgebracht werden, wie zum Beispiel auf dem hinteren Vorsatz des Passes der Vereinigten Arabischen Emirate. Dies ergibt einen gleichmäßigen Fluoreszenzfarbverlauf von Grün über Rot zurück zu Grün.

ABBILDUNG 10: UV-FLUORESZIERENDE FARBEN



Bi-fluoreszierende Farben erscheinen nur unter mindestens zwei unterschiedlichen UV-Lichtquellen verschiedenfarbig, zum Beispiel unter UV-A- und UV-C-Strahlen.

ABBILDUNG 11: BI-FLUORESZIERENDE FARBEN



IR-Effektfarben weisen nur unter IR-Beleuchtung unterschiedliche Charakteristika auf. Entweder sie absorbieren das Infrarotlicht gezielt, was die Farben sichtbar werden lässt, oder sie sind IR-transparent und zeigen somit keine Farben. Diese Farbart eignet sich hervorragend, um personalisierte Daten vor Verfälschungen zu schützen.

ABBILDUNG 12: IR-EFFEKTFARBEN

Up-Conversion- oder auch „Anti-Stokes"-Pigmente wandeln, im Gegensatz zu den UV-fluoreszierenden Farben, unsichtbares langwelliges Licht in sichtbares Licht um. Merkmale, die mit dieser Farbe aufgebracht wurden, lassen sich zumeist mit IR-Laser erkennen.

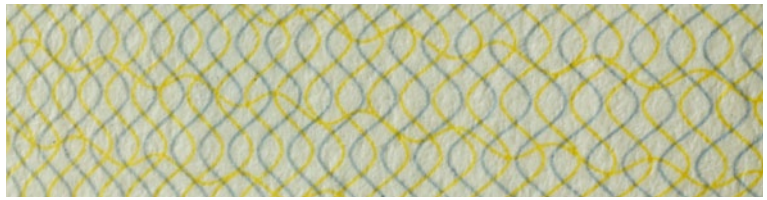
Alle Farben können sowohl in papierbasierten Dokumenten als auch in PC-Datenseiten eingesetzt werden. **Level-3-Effektfarben** erschweren die Totalfälschung eines Passes und können nur mithilfe forensischer Hilfsmittel ausgelesen werden. Die eigens in der Bundesdruckerei entwickelte Fluoreszenzfarbe **Innosec Colour CX** ermöglicht zum Beispiel eine spektrale Umverteilung des ausgestrahlten Lichts, sodass eine Art individueller „Fingerprint" entsteht. **Innosec Colour CX** bietet damit viele unterschiedliche und vor allem kundenindividuelle Codierungsvarianten.

ABBILDUNG 13: INNOSEC COLOUR CX

Drucktechnische Anwendungsformen

Verschiedene Druckmotive hinterlassen einmalige Muster und Raster, die Reisedokumente vor Kopien schützen. Eine Erfindung aus dem 17. Jahrhundert, die **Guillochen,** wird heute noch für moderne Reisepässe eingesetzt. Die Ziermuster bestehen aus feinen Linien, die kunstvoll ineinander verschlungen sind. Der Betrachter kann Guillochen mit bloßem Auge oder – wenn die Linien mit fluoreszierenden Farben gedruckt sind – mithilfe von UV-Licht erkennen. Guillochen können auch mehrfarbig sein.

ABBILDUNG 14: GUILLOCHEN



Im sogenannten **Irisdruckverfahren** verwendet der Drucker zwei oder mehr Farben, die fließend ineinander übergehen. Dieser Farbverlauf ist durch genaue Betrachtung zu erkennen und bietet in Verbindung mit UV-sichtbaren Farben einen hohen Schutz gegen Kopien oder Totalfälschungen.

ABBILDUNG 15: IRISDRUCKVERFAHREN

Anti-Kopier-Muster sind versteckte Informationen, die im Untergrunddruck eingebettet und mit bloßem Auge nicht zu erkennen sind. Beim Kopieren rufen sie sogenannte Interferenzmuster hervor, die sich eindeutig vom Original unterscheiden.

ABBILDUNG 16: ANTI-KOPIER-MUSTER

Linienraster erzeugen ein Bild im Hintergrund, dessen Linien bei einem Kopierversuch aufeinander zulaufen und so zu störenden Bildelementen führen.

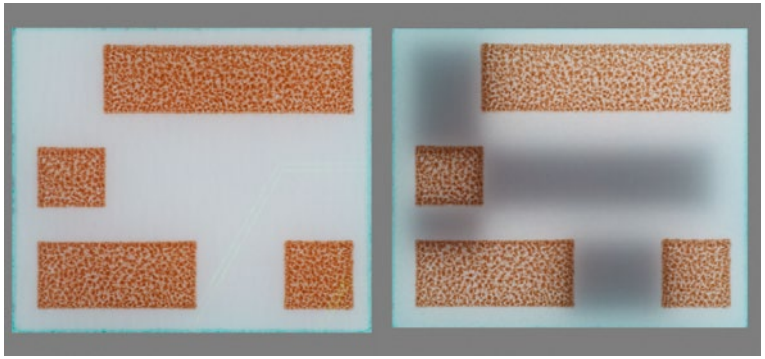
ABBILDUNG 17: LINIENRASTER

Eine spezielle Form des Rasters ist das **Motivraster.** Geometrische Figuren und/oder Buchstaben stellen Bilder dar, die bei einem Kopierversuch grob pixelig werden. Weit verbreitet ist das Aufdrucken einer **Mikroschrift.** Sie kann positiv oder negativ gedruckt sein und besteht aus winzigen Buchstaben, Zahlen, Motiven oder Symbolen von 0,25 bis 0,5 Millimetern Höhe. Lesbar sind Mikroschriften nur mithilfe einer Lupe. Mikroschriften erschweren Kopierversuche und Verfälschungen von Sicherheitsdokumenten.

ABBILDUNG 18: MIKROSCHRIFT POSITIV

Vor Totalfälschungen schützt zudem das **Durchsichtsregister:** Dabei werden Teile eines Motivs so auf Vorder- und Rückseite einer Seite aufgedruckt, dass der Betrachter das vollständige Motiv erst im Durch- oder Gegenlicht erkennen kann.

ABBILDUNG 19: DURCHSICHTSMERKMAL

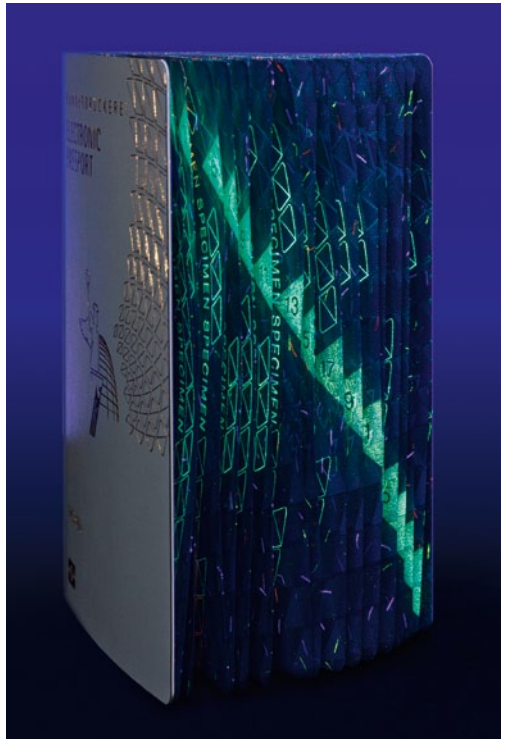


Alle genannten Sicherheitsmerkmale sind sowohl für Papier als auch für Polycarbonat geeignet. Weitere Merkmale, die nur auf den Innen- bzw. Visaseiten verwendet werden, sind **integrierte Seitenzahlen** und **Flattermarken.** Die integrierten Seitenzahlen bestehen zum Beispiel aus Guillochen oder speziellen Rastern, sodass Einzelseiten nicht mehrfach kopiert werden können.

ABBILDUNG 20: INTEGRIERTE SEITENZAHLEN

Spezielle Markierungen oder Zeichen, die mitunter nur unter einer UV-Lichtquelle erkennbar sind, bilden Flattermarken, die beim Betrachten des Passbuchrandes durch das ganze Buch wandern. Dadurch wird ein unbemerktes Austauschen oder Heraustrennen einzelner Seiten verhindert. Beide Merkmale schützen das Passbuch vor Kopie und Verfälschung.

ABBILDUNG 21: FLATTERMARKE UNTER UV-LICHTQUELLE

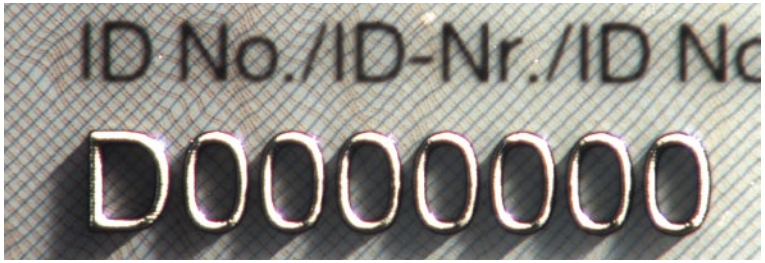


Haptische und mechanische Anwendungsformen
Bei diesen Verfahren verändern Laser oder Prägeformen die Oberfläche des Trägermaterials des Passes so, dass sich Bilder und Texte erfühlen lassen. Fachleute unterscheiden zwischen auf- und abtragenden sowie durchdringenden Ausprägungen. Auf- beziehungsweise abtragende Prägungen auf der Oberfläche von Dokumenten sind deutlich fühlbar. Sie werden mithilfe unterschiedlicher Verfahren erstellt, je nachdem, ob das Trägermaterial aus Papier oder PC besteht. Dazu gehören unter anderem die **Heißfolienprägung** für den Einband des Passbuches, die **Hoch-/Tiefprägung** sowie die **taktile Lasergravur** für PC-Dokumente und der **Stichtiefdruck** für Papier. Beim Heißfoliendruck wird mit einem heißen Stempel ein Motiv aus goldfarbener Folie auf das Cover des Passbuches übertragen und gleichzeitig eingeprägt. Ein Beispiel dafür ist der Bundesadler auf der Vorderseite des deutschen Reisepasses.

ABBILDUNG 22: HEISSFOLIENPRÄGUNG

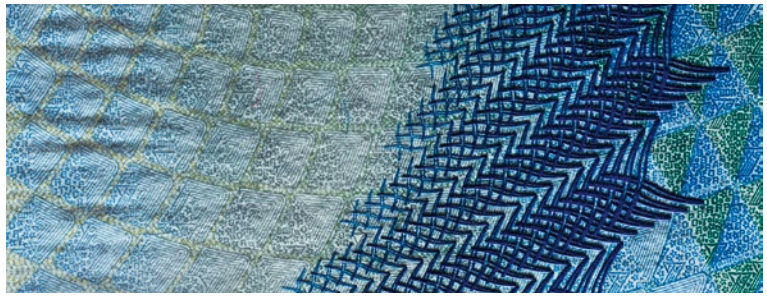
Fühlbare Oberflächenprägungen können mithilfe von Hoch- oder Tiefprägungen oder einer Kombination aus beiden Verfahren erstellt werden. Taktile Lasergravuren, wie sie auf der Datenseite des luxemburgischen Passes zum Einsatz kommen, werden mithilfe eines Lasers in das PC-Dokument eingraviert. Dabei wird die Oberfläche des Dokuments so verändert, dass die Gravuren erhaben und somit deutlich fühlbar sind.

ABBILDUNG 23: TAKTILE LASERGRAVUR



Auf Papier lässt sich ein ähnlicher Effekt mithilfe des Stichtiefdruckverfahrens erreichen: Die hohen Farbschichten auf dem Bedruckstoff kann man deutlich fühlen. Außerdem lassen sich mithilfe dieses Verfahrens latente Bilder erstellen. Durch Kippen des Dokuments kann der Betrachter zusätzliche Bilder, Schriften oder Logos erkennen, die häufig mit Sonderfarben, wie OVI (optisch variable Farben), aufgebracht sind.

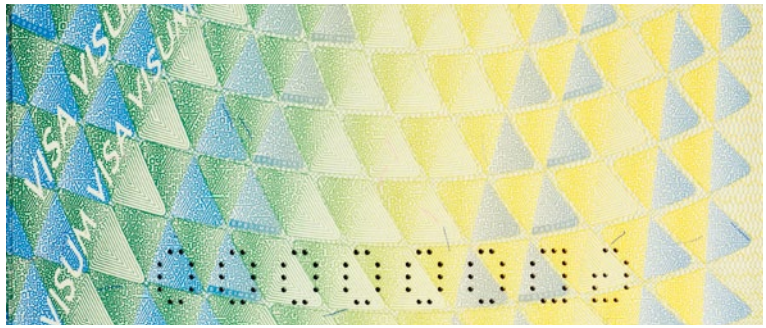
ABBILDUNG 24: LATENTE BILDER



Mit Ausnahme des Heißfoliendrucks schützen alle Verfahren die Dokumente vor Kopierversuchen und Verfälschungen. Motive, die mithilfe des Heißfoliendruckverfahrens erstellt werden, schützen den Einband des Passes nur vor Kopierversuchen.

Zu den sogenannten durchdringenden Merkmalen gehören die **konische Laserperforation** für Dokumente aus Papier und die **Imageperforation,** die für Papier und PC-Dokumente geeignet ist. Die Seitennummern auf den Inhaltsseiten des Passbuchs werden zum Beispiel mithilfe der konischen Laserperforation erstellt. Dabei nimmt der Durchmesser der erzeugten Löcher von der ersten Inhaltsseite bis zum hinteren Cover kontinuierlich ab, die Löcher laufen konisch zu.

ABBILDUNG 25: KONISCHE LASERPERFORATION

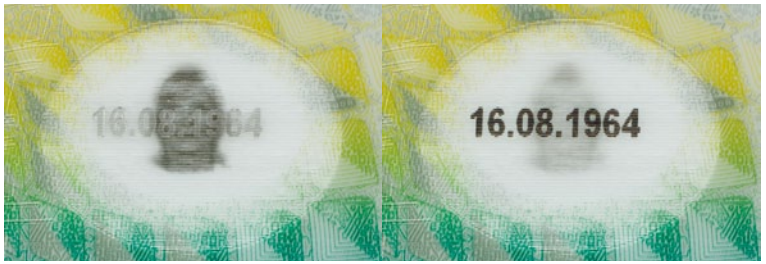


Bei der Imageperforation brennt ein Laser kleine Löcher in das Dokument, die Bilder, Zeichen oder Logos ergeben. Beide Perforationsarten sind sicht- und fühlbar und bieten Schutz vor Kopie und Verfälschung.

ABBILDUNG 26: IMAGEPERFORATION

Die **Changeable** oder **Multiple Laser Images (CLI/MLI)** stellen eine besondere Form der haptischen und mechanischen Anwendungsformen dar und können nur auf PC-Dokumenten eingesetzt werden. Auf der Oberfläche der PC-Datenseite werden während der Lamination Linsen integriert. In diese schreibt ein Laser in unterschiedlichen Winkeln verschiedene Informationen ein. Je nach Blickwinkel sieht der Betrachter jeweils andere Darstellungen, zum Beispiel Fotos, Logos oder auch Personendaten. Dieses Sicherheitsmerkmal ermöglicht es, personenindividuelle Daten des Karteninhabers auf besonders sichere Weise vor Kopien sowie Verfälschungen zu schützen.

ABBILDUNG 27: CLI/MLI



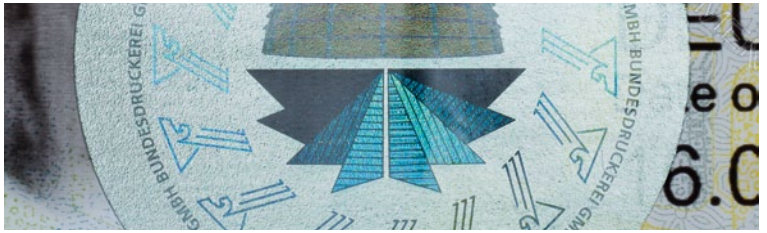
Folien und Overlays

Neben den Sicherheitsmerkmalen, die in oder auf dem Passbuch angebracht sind, schützen sogenannte Folien und Overlays zusätzlich die Personendaten auf der Datenseite des Passes. Folien und Overlays können vollflächig oder partiell auf oder in der Datenseite verwendet werden. **Hologrammfolien** zum Beispiel sind transparente Folien, die kinematisch-holografische Strukturen enthalten und vollflächig auf die Dokumentenoberfläche aufgebracht sind.

ABBILDUNG 28: HOLOGRAMMFOLIE

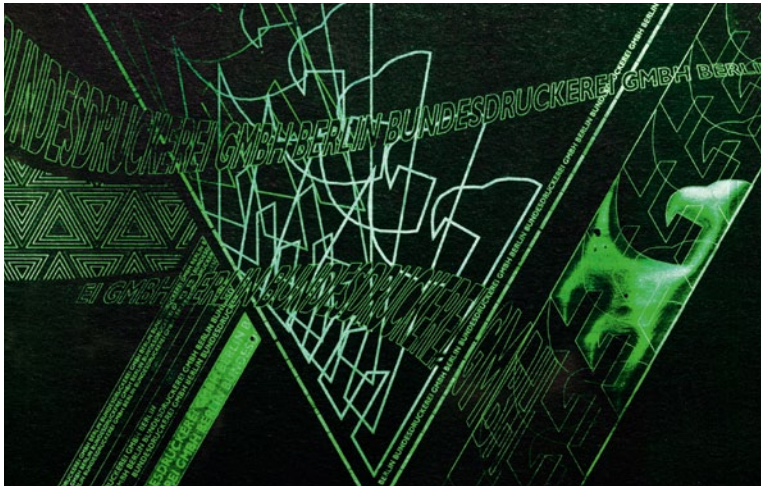
Das **innenliegende Hologramm** hingegen befindet sich, wie der Name schon sagt, innerhalb des PC-Dokumentenaufbaus und schützt das Lichtbild des Inhabers. Es hat eine kinematische Struktur und kann maschinenprüfbare Elemente enthalten.

ABBILDUNG 29: INNENLIEGENDES HOLOGRAMM



Ein weiteres Sicherheitsmerkmal, das aufgrund seiner kinematischen Strukturen zum Schutz von Papier- und PC-Dokumenten zum Einsatz kommt, ist das **Volumenhologramm.** Das Besondere am Volumenhologramm ist, dass die holografischen Informationen nur unter einem bestimmten Betrachtungswinkel sichtbar sind. Im deutschen Pass werden zum Beispiel der Bundesadler, das Lichtbild des Passinhabers und die maschinenprüfbaren Zeilen holografisch wiedergegeben. Volumenhologramme sind sehr schwer zu fälschen, sie schützen vor Kopie, Verfälschung und Totalfälschung. Die deutschen ID-Dokumente wie Ausweis, Pass und Führerschein sind daher durch Volumenhologramme geschützt.

ABBILDUNG 30: VOLUMENHOLOGRAMM



Einklang von Design und Sicherheit

Viele der genannten Sicherheitsmerkmale lassen sich miteinander kombinieren, um die Sicherheit von Reisepässen zu erhöhen. Dabei sollten sowohl die Sicherheitsmerkmale als auch das Design der Dokumente die Richtlinien der ICAO erfüllen. Die Herausforderung liegt darin, beides in Einklang zu bringen. Zum einen sind Pässe und ePässe quasi die Visitenkarte des Landes, das sie ausgibt. Zum anderen erfordern neue nationale und internationale Richtlinien eine permanente Weiterentwicklung von Sicherheitsmerkmalen, die unter Umständen das Aussehen der Pässe verändern.

Im Trend: leicht zu prüfende Merkmale

Bei Grenzkontrollen müssen Dokumente auch ohne technische Hilfsmittel und möglichst schnell auf ihre Echtheit überprüft werden können. Der Trend geht deshalb zu Level-1-Merkmalen, die Grenzbeamte besonders einfach und sicher erkennen können. Viele der genannten Sicherheitsmerkmale lassen sich mit bloßem Auge erkennen, seien es Sicherheitsfäden, optisch variable Farben, Guillochen oder innenliegende Hologramme. Auch durch die mehrfache Aufbringung von Daten in unterschiedlichen Verfahren, z. B. als Lasergravur und als individuelles Hologramm, wird die Überprüfung erleichtert. Die Beratung zur optimalen Auswahl und Zusammenstellung der Merkmale gehört zu den Kernkompetenzen der Bundesdruckerei.

FUNKTION UND NIVEAU DER SICHERHEITS-MERKMALE AUF EINEN BLICK

Sicherheitsmerkmal	Kurzbeschreibung	Einsatzbereich	Schutz vor	Prüflevel	Prüfmethode	ICAO	Integriert in ePass
Substrate							
Papier	Träger für Sicherheitsdruck, enthält Sicherheitsmerkmale	Papier	Kopie Verfälschung Totalfälschung	Level 1 Level 2 Level 3	Visuell, Durchlicht Mit Hilfsmitteln Forensisch	ICAO	Vorsatz, Datenseite Papier, Inhaltsseiten
Polycarbonat	Extrem widerstandsfähig, Karten bestehen aus mehreren Schichten	Polycarbonat	Kopie Verfälschung Totalfälschung	Level 1 Level 2 Level 3	Visuell, Durchlicht Mit Hilfsmitteln Forensisch	ICAO	Datenseite PC
Melierfasern	Sicherheitsfasern, die unter das Substrat gemischt werden	Papier Kunststoff	Kopie Totalfälschung	Level 1 Level 2	Visuell UV-Lampe	ICAO	Vorsatz, Datenseite PC + Papier, Inhaltsseiten
Chemische Reagenzien	Machen Manipulationsversuche durch Ändern oder Ausbluten von Farben sichtbar	Papier	Verfälschung	Level 1	Visuell Prüfstift	ICAO	Vorsatz, Datenseite PC + Papier, Inhaltsseiten
Wasserzeichen	Unterschiedliche Faserdichten im Papier bilden Motive	Papier	Kopie Totalfälschung	Level 1	Visuell	ICAO	Datenseite Papier, Inhaltsseiten
Heftfaden	Bestehen aus mehreren Kunststoff- oder Baumwolladern, spezielles Nähverfahren	Passbuch mit PC- und Papierdatenseite	Totalfälschung	Level 1 Level 2	Visuell UV-Lampe	ICAO	Datenseite PC + Papier, Inhaltsseiten
Sicherheitsfaden	Bestehen aus Metall oder Kunststoff, werden in oder auf dem Substrat angebracht, große Bandbreite	Papier Kunststoff	Kopie Totalfälschung	Level 1 Level 2	Visuell UV-Lampe Maschinell	ICAO optional	Datenseite PC + Papier, Inhaltsseiten
Farben							
Optisch variable Farben (OVI)	Enthalten Pigmente, die je nach Betrachtungswinkel die Farbe ändern	Papier Kunststoff	Kopie	Level 1	Visuell	ICAO optional	Vorsatz, Datenseite PC + Papier, Inhaltsseiten
Irisierende Farben	Enthalten transparente Pigmente aus winzigen Glimmerplättchen, schimmern perlmuttartig	Papier Kunststoff	Kopie	Level 1	Visuell	ICAO optional	Vorsatz, Datenseite PC + Papier, Inhaltsseiten
Thermochromatische Farben	Farbmittel reagieren auf Temperaturunterschiede	Papier Kunststoff	Kopie	Level 1	Visuell durch Temperaturveränderung	–	Vorsatz, Datenseite PC + Papier, Inhaltsseiten
UV-fluoreszierende Farben	Farben emittieren unter UV-Lampen ein visuell sichtbares Spektrum	Papier Kunststoff	Kopie	Level 2	UV-Lampe VISOTEC 300	ICAO	Vorsatz, Datenseite PC + Papier, Inhaltsseiten
Bi-fluoreszierende Farben	Erscheinen unter zwei UV-Quellen farbig	Papier Kunststoff	Kopie	Level 2	UV-Lampe mit unterschiedlichen Wellenlängen	ICAO optional	Vorsatz, Datenseite PC + Papier, Inhaltsseiten
IR-Effektfarben	Weisen unter IR-Beleuchtung unterschiedliche Charakteristika auf	Papier Kunststoff	Kopie Verfälschung	Level 2	IR-Quelle + IR-Kamera VISOTEC 300	ICAO	Vorsatz, Datenseite PC + Papier, Inhaltsseiten

Sicherheitsmerkmal	Kurzbeschreibung	Einsatzbereich	Schutz vor	Prüflevel	Prüfmethode	ICAO	Integriert in ePass
Innosec Colour CX	Spektrale Verteilung des Lichts ermöglicht das Auslesen eines „Fingerprints“	Papier Kunststoff	Kopie Totalfälschung	Level 2 Level 3	UV-Lampe Spektrometer	–	Vorsatz, Datenseite PC + Papier, Inhaltsseiten
Up-Conversion	Pigmente wandeln unsichtbares langwelliges Licht in sichtbares Licht um	Papier Kunststoff	Kopie	Level 2	Visuell IR-Laser	ICAO optional	Vorsatz, Datenseite PC + Papier, Inhaltsseiten
Drucktechnische Anwendungsformen							
Guillochen	Ziermuster aus feinen ineinander verschlungenen Linien	Papier Kunststoff	Kopie Verfälschung	Level 1	Visuell Lupe	ICAO	Vorsatz, Datenseite PC + Papier, Inhaltsseiten
Irisdruck	Einfärbeverfahren, bei dem zwei oder mehr Farben fließend ineinander übergehen	Papier Kunststoff	Kopie	Level 1 Level 2	Visuell UV-Lampe	ICAO	Vorsatz, Datenseite PC + Papier, Inhaltsseiten
Anti-Kopier-Muster	Im Untergrunddruck versteckte Informationen	Papier Kunststoff	Kopie	Level 1	Visuell Lupe	ICAO	Vorsatz, Datenseite PC + Papier, Inhaltsseiten
Linienraster	Erzeugen Bild im Hintergrund	Papier Kunststoff	Kopie	Level 2	Visuell Lupe	ICAO	Vorsatz, Datenseite PC + Papier, Inhaltsseiten
Motivraster	Verwenden geometrische Formen und/oder Buchstaben zur Darstellung gerasterter Bilder	Papier Kunststoff	Kopie	Level 2	Visuell Lupe	ICAO	Vorsatz, Datenseite PC + Papier, Inhaltsseiten
Mikroschrift/-text	Besteht aus winzigen Zahlen, Buchstaben, Motiven oder Symbolen	Papier Kunststoff	Kopie Verfälschung	Level 2	Visuell Lupe	ICAO	Vorsatz, Datenseite PC + Papier, Inhaltsseiten
Integrierte Seitenzahlen	Seitennummerierung durch Guillochen, spezielle Raster usw.	Papier	Kopie Verfälschung	Level 1	Visuell Lupe	ICAO optional	Inhaltsseiten
Durchsichtsregister	Abbildungen, die nur im Durchlicht zu sehen sind	Papier Kunststoff	Kopie Totalfälschung	Level 1	Visuell	ICAO optional	Datenseite PC + Papier, Inhaltsseiten
Flattermarke	Spezielle Markierungen, die durch das Passbuch „wandern“	Papier	Kopie Verfälschung	Level 1 Level 2	Visuell UV-Prüfung	–	Inhaltsseiten
Haptische Anwendungsformen							
Heißfolienprägung	Einprägen eines Motivs auf den Einband mit heißem Stempel	Einband	Kopie	Level 1	Visuell Haptisch	ICAO optional	Einband
Stichtiefdruck	Überträgt hohe Farbschichten auf Bedruckstoff	Papier	Kopie Verfälschung	Level 1	Visuell Haptisch	ICAO optional	Vorsatz, Inhaltsseiten
Latente Bilder	Werden im Stichtiefdruck gedruckt, je nach Betrachtungswinkel erscheinen zusätzliche Informationen wie Texte, Symbole, Logos	Papier	Kopie Totalfälschung	Level 1	Visuell im Streiflicht Lupe	ICAO optional	Vorsatz, Inhaltsseiten

Sicherheitsmerkmal	Kurzbeschreibung	Einsatzbereich	Schutz vor
Konische Laserperforationen	Der Durchmesser der erzeugten Löcher nimmt kontinuierlich ab	Papier	Kopie
Hoch-/Tiefprägung	Fühlbare Prägungen	Kunststoff	Kopie Verfälschung
Taktile Lasergravuren	Eingravieren von Bildern und Text mithilfe von Lasern	Kunststoff	Kopie Verfälschung
Imageperforationen	Perforationen erzeugen Bilder, Zeichen oder Logos	Papier Kunststoff	Kopie Verfälschung
Changeable Laser Images	Laserbilder, die sich je nach Blickwinkel ändern	Kunststoff	Kopie Verfälschung
Folien und Overlays			
Hologrammfolien	Transparente Folien, die kinematisch-holografische Figuren enthalten	Papier	Kopie Verfälschung Totalfälschung
Innenliegende Hologramme	Holografische Strukturen, basierend auf metallisierter oder demetallisierter Folie, eingebettet in den Kartenaufbau (Regenbogeneffekt)	Kunststoff	Kopie Verfälschung Totalfälschung
Volumenhologramme	Oberflächlich aufgebrachte holografische Folien, mit in das Materialvolumen geschriebener Information, einfarbig/mehrfarbig möglich	Kunststoff	Kopie Verfälschung Totalfälschung

Prüflevel	Prüfmethode	ICAO	Integriert in ePass
Level 1	Visuell Haptisch	ICAO	Inhaltsseiten, Vorsatz und Einband hinten
Level 1	Visuell Haptisch	ICAO optional	Datenseite PC
Level 1	Visuell im Streiflicht Haptisch	ICAO	Datenseite PC
Level 1	Visuell Haptisch	ICAO	Datenseite PC + Papier
Level 1	Visuell Haptisch	ICAO	Datenseite PC
Level 1 Level 2	Visuell Maschinell	ICAO optional	Datenseite Papier
Level 1	Visuell	ICAO optional	Datenseite PC
Level 1 Level 2 Level 3	Visuell Maschinell	–	Datenseite PC + Papier

KAPITEL 4
DER CHIP ALS TRESOR DES ePASS

Was den integrierten Chip auszeichnet – und wie er in hochsichere ID-Systeme eingebunden ist

Der Chip enthält die auf dem Pass aufgedruckten Informationen in digitaler Form. Um eine noch festere Bindung zwischen Inhaber und Dokument herzustellen, sollten gemäß ICAO und EU zudem biometrische Daten darauf gespeichert sein – etwa das für die automatische Gesichtserkennung geeignete Lichtbild des Inhabers oder seine Fingerabdrücke. Die entsprechenden Datensätze werden auf dem Chip des Ausweisdokuments gespeichert und kryptografisch gesichert. Zusätzlich signiert der ausstellende Staat die gespeicherten Daten digital und kennzeichnet sie damit als authentisch und unverfälscht. Bei der Kontrolle wird dann der auf dem Chip hinterlegte Fingerabdruck mit dem Lebendabdruck des Ausweisinhabers verglichen. Wenn es die Datenschutzrichtlinien des ausstellenden Staats zulassen, können biometrische Daten zusätzlich in zentralen Datenbanken hinterlegt werden, um einen zuverlässigen, automatisierten Vergleich zu ermöglichen.

Für Reisepässe schreibt die ICAO kontaktlose Speichermedien vor. Diese Chips haben eine längere Lebensdauer als kontaktbehaftete Chips oder Hybridmodelle. Zudem können kontaktlose Chips weniger leicht beschädigt werden. Sie verfügen über keine eigene Energiequelle, sondern erhalten ihre Energie erst aus dem elektromagnetischen Feld des Lesegeräts. Der Chip kann daher nur dann Daten übertragen, wenn er sich in der Nähe eines Lesegeräts befindet und aktiviert wurde. Oberstes Gebot bei Reisepässen ist der Schutz vor missbräuchlichem Zugriff auf den Chip als Träger sensibler Daten. Deshalb wird das Reisedokument in eine sogenannte Public-Key-Infrastruktur (PKI) eingebunden, ein System, das digitale Zertifikate ausstellen, verteilen und prüfen kann. Nur wer eine entsprechende gültige hoheitliche Berechtigung besitzt, kann zum Beispiel die Fingerabdruckdaten aus dem Speichermedium auslesen. Die Zertifikate sichern die Kommunikation zwischen Chip und verschiedenen Endgeräten wie PCs, Lesegeräten oder Änderungsterminals ab. Hoheitliche Ausweisdokumente wie der Reisepass setzen eine Einbindung in hoheitliche PKI voraus. Die Experten der Bundesdruckerei kennen die Anforderungen und unterstützen ihre Partner bei der Implementierung.

Sicherheitsmechanismen eines Chips laut ICAO

Um die Chips bestmöglich zu sichern und um zu gewährleisten, dass sie in unterschiedlichen IT-Systemen funktionieren, hat die ICAO verschiedene Standardverfahren und Sicherheitsmerkmale definiert.

> Die auf dem Chip hoheitlicher, international verwendbarer Reisedokumente gespeicherten Daten müssen einer standardisierten, logischen Datenstruktur (LDS) folgen, die eine Reihe obligatorischer und optionaler Datenelemente enthält. Verpflichtend ist die Nutzung der Datengruppe DG1, einer digitalen Version der gedruckten maschinenlesbaren Zone mit biografischen Daten des Inhabers, Dokumentennummer und Ablaufdatum. Ebenfalls vorgeschrieben ist die Datengruppe DG2, die das biometrische Gesichtsbild enthält. Alle anderen Datenelemente sind optional.

> Um den Chip vor unbefugten Zugriffen zu bewahren, empfiehlt die ICAO das als Basic Access Control (BAC) bezeichnete Zugriffsprotokoll, das fast alle Länder für ihre Reisepässe einsetzen. BAC schützt insbesondere vor Lauschangriffen und dem so genannten Skimming, dem heimlichen Auslesen von Speichermedien mittels verborgener Lesegeräte. Dafür generiert BAC mithilfe eines komplexen kryptografischen Verfahrens einen Schlüssel aus den Daten der maschinenlesbaren Zone (MRZ). Mit diesem Schlüssel muss sich das Lesegerät gegenüber dem Chip authentisieren. Dafür schickt der Chip dem Lesegerät eine Zufallszahl. Das Gerät verschlüsselt diese Zahl mit dem Zugriffsschlüssel und sendet sie zurück an das Speichermedium. Erst danach werden die Daten zum Auslesen freigegeben. Bei den mit dem BAC-Protokoll gesicherten Daten handelt es sich um die Informationen, die auch auf dem Reisepass abgedruckt sind – also Gesichtsbild, Name oder Geburtsdatum. Um BAC noch sicherer zu machen, sollen ab Dezember 2014 alle auszugebenden elektronischen Pässe über das sogenannte Supplemental Access Control (SAC) verfügen. Bei diesem Sicherheitsprotokoll kommt das Verfahren Password Authenticated Connection Establishment (PACE) zum Einsatz. Es stellt sicher, dass der kontaktlose Chip erst nach Ein-

gabe der auf dem Ausweis verzeichneten Card Access Number (CAN) zum Auslesen freigeschaltet wird.

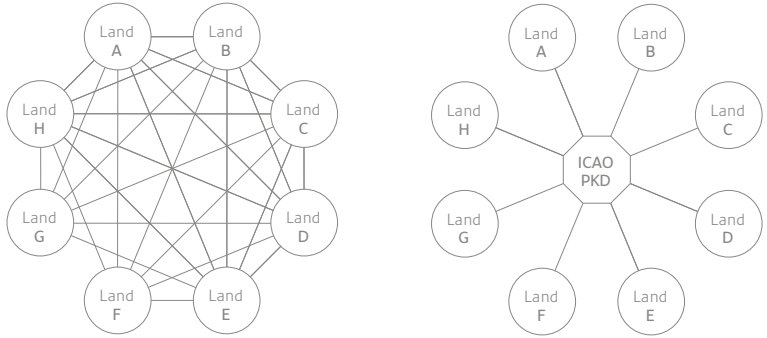
> Der Chip muss den Sicherheitsmechanismus der sogenannten Passiven Authentisierung (PA) unterstützen. Dieser beinhaltet im Wesentlichen eine digitale Signatur der Hashwerte aller auf dem Chip gespeicherten Datengruppen. Die Signatur erzeugt der Document Signer, in der Regel der Hersteller des Ausweisdokuments, während der Personalisierung des Chips.

> Damit die Passive Authentisierung funktioniert, hat die ICAO eine Public-Key-Infrastruktur definiert, die aus zwei Arten von Zertifikaten besteht. Die Zertifikate der obersten Ebene der PKI-Hierarchie heißen Country Signing Certificates (CS). Sie werden von der nationalen Wurzelinstanz ausgestellt, der sogenannten Country Signing Certification Authority (CSCA). In Deutschland ist das Aufgabe des Bundesamts für Sicherheit in der Informationstechnik (BSI). Daneben gibt es Document Signer Certificates (DS). Die DS-Zertifikate werden mit dem Wurzelzertifikat der ausstellenden Nation signiert. Mit ihnen signiert der offiziell beauftragte Passhersteller wiederum die auf dem Chip gespeicherten Daten. Auf diese Weise entsteht eine Zertifikatskette, über die zurückverfolgt werden kann, ob die gespeicherten Daten tatsächlich von der ausstellenden Nation stammen.

ABBILDUNG 31: PKI FÜR PASSIVE AUTHENTISIERUNG

> Da die CS-Zertifikate der Vertrauensanker in der PKI-Hierarchie sind, werden sie auf diplomatischem Weg an andere Länder und an die ICAO übermittelt. Um Zeit und Kosten zu sparen, ist dies aber nur einmal nötig – zu Beginn einer Kooperation. Anschließend können die teilnehmenden Staaten ihre Zertifikate über das Public Key Directory (PKD) der ICAO übermitteln. Damit die Kooperationsstaaten sicher sein können, dass die über das PKD ausgetauschten Zertifikate authentisch sind, wird ein neues CS-Zertifikat mit dem Schlüssel des alten CS-Zertifikats signiert. Es heißt deshalb auch Link-Zertifikat. Über das PKD können Grenzbehörden zudem DS-Zertifikate beziehen und anhand von Sperrlisten prüfen, ob bestimmte Zertifikate zurückgezogen und damit als ungültig gemeldet wurden. Derzeit beteiligten sich rund 35 Länder am PKD. Ziel ist es, diese Plattform zum Austausch von Zertifikaten weiter auszubauen. Zudem wird darüber diskutiert, ob das PKD künftig auch den Zugriff auf zusätzlich auf dem Chip gespeicherte Informationen wie Visa sichern kann.

ABBILDUNG 32: ICAO PKD



Ohne zentrale Vermittlungsstelle müssten 8 Staaten 56 bilaterale Kontakte pflegen, um ihr Zertifikat zu übermitteln (Bild links). Das PKD vereinfacht den Austausch erheblich (Bild rechts).

Die Vorteile des PKD im Überblick

> Über das PKD kann die Echtheit der auf dem Chip gespeicherten Daten schnell und zuverlässig geprüft werden.

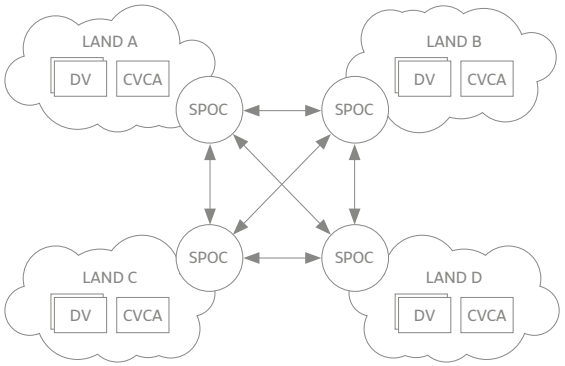
> Die ICAO kontrolliert jedes Zertifikat, bevor es im PKD veröffentlicht wird. Gefälschte Zertifikate geraten so gar nicht erst in Umlauf.

> Staaten, die ihre Zertifikate bisher nur mit einigen wenigen Staaten auf diplomatischem Weg ausgetauscht haben, profitieren von sogenannten Masterlisten. Diese werden ebenfalls über das PKD ausgetauscht und führen alle CSCA-Zertifikate auf, denen eine Nation vertraut. So sind auf der Masterliste Deutschlands zum Beispiel die Zertifikate von Ländern wie Frankreich und Italien verzeichnet. Möchte ein Staat also unkompliziert selbst eine Liste vertrauenswürdiger Zertifikate anlegen, kann er sie über die Masterliste eines Kooperationsstaates erstellen.

Speziell um die besonders sensiblen biometrischen Daten wie den Fingerabdruck auf dem Chip zu schützen, ist eine erweiterte Zugangskontrolle notwendig: die sogenannte Extended Access Control (EAC). Verpflichtend ist EAC bislang allerdings nur in den Ländern der Europäischen Union. Dieses Sicherheitsprotokoll gibt vor, dass sich zunächst der Chip am Dokumentenlesegerät authentisieren muss. Dieses Verfahren nennt sich Chip Authentication (CA) und dient indirekt auch als Schutz vor Versuchen, die Inhalte des Chips zu klonen. Im zweiten Schritt authentisiert sich das Lesegerät mit einem Berechtigungszertifikat beim Chip (Terminal Authentication, TA). Erst danach erhält es Zugriff auf den auf dem Chip gespeicherten Fingerabdruck.

Für EAC-Zertifikate gibt es auf europäischer Ebene keine zentrale Verteilerstelle wie das PKD. Um den Austausch der Zertifikate zu erleichtern, wurde ein technischer Standard namens SPOC (Single Point of Contact) entwickelt. Demnach übermittelt jede Nation ihre Berechtigungszertifikate über einen eigenen, zentralen SPOC-Server. In den meisten Fällen ist dieser bei der Country Verifying Certificate Authority (CVCA) eines Landes angesiedelt. Ihre Aufgabe ist es, Zugriffsrechte für sogenannte Document Verifier Certificate Authorities (DVCA) zu erteilen. Die DVCA sind wiederum dazu autorisiert, Berechtigungszertifikate für nationale Terminals auszugeben – etwa in Ausweisbehörden oder an Grenzkontrollen. Der SPOC-Server übernimmt die Kommunikation der CVCA und der DVCA eines Landes mit denen anderer Nationen. So wird zum Beispiel verhindert, dass die zahlreichen Grenzkontrollen eines Landes die Erlaubnis zum Auslesen der biometrischen Daten einzeln bei der CVCA einer anderen Nation anfragen müssen.

ABBILDUNG 33: SPOC-SCHEMA

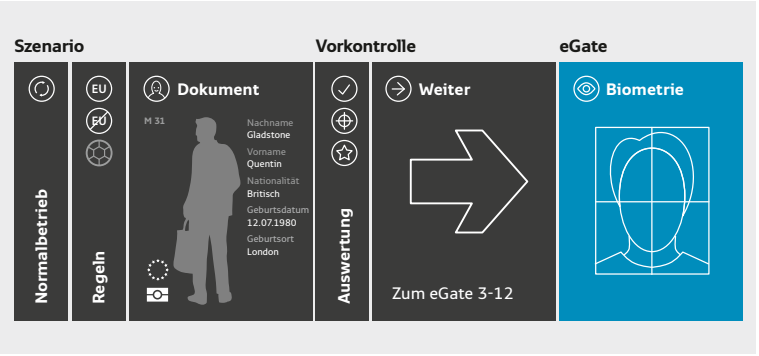


Die Kommunikation mit der ausländischen Country Verifying Certificate Authority (CVCA) und den ausländischen Document-Verifier-Instanzen (DV) findet zwischen dem nationalen SPOC und dem SPOC der ausländischen EAC-PKI statt.

AUTOMATISIERTE KONTROLLE VON ELEKTRONISCHEN REISEPÄSSEN

Der elektronische Reisepass trägt nicht nur zu mehr Sicherheit, sondern auch zu einer komfortablen und zeitsparenden Abfertigung an Grenzkontrollen bei. Mit ihm können Reisende sogenannte eGates passieren und die Kontrolle selbstständig durchführen. Dazu muss der Reisepass lediglich auf das Lesegerät am eGate gelegt werden. Innerhalb von Sekunden wird das Dokument ausgelesen und auf Echtheit geprüft. Zeitgleich können Zusatzprüfungen durchgeführt werden. So ist es zum Beispiel möglich, Datenbankabfragen vorzunehmen oder das auf dem Pass gespeicherte biometrische Foto mit einem vor Ort erstellten Echtbild des Reisenden zu vergleichen. In Zeiten mit großem Passagieraufkommen – etwa im Vorfeld großer Sportveranstaltungen – können eGates besonders nützlich sein. So könnten an europäischen Flughäfen Kontrollen parallel stattfinden: Während EU-Bürger eGates passieren, würden Reisende aus anderen Ländern durch Grenzbeamte abgefertigt.

ABBILDUNG 34: PROZESS DER AUTOMATISIERTEN GRENZKONTROLLE



In Großbritannien gibt es bereits an mehreren Flughäfen automatisierte Grenzkontrollen. Seit 2004 testet auch der größte Flughafen Deutschlands in Frankfurt am Main unterschiedliche Verfahren. In den kommenden Jahren ist mit einer stetigen Weiterentwicklung und Standardisierung von elektronischen Grenzkontrollen zu rechnen. Derzeit wird beispielsweise an einer technischen Spezifikation für die Nutzung biometrischer Daten an eGates gearbeitet. Erste Vorschläge sollen 2013 bekannt gegeben werden.

KAPITEL 5
VON DER KONZEPTION BIS ZUR VERIFIKATION

Wie ein ePass entsteht und gehandhabt wird – und wie die Bundesdruckerei diesen Prozess begleitet

Reisepässe sind, wie im vorangegangenen Kapitel erläutert, in hochkomplexe ID-Systeme eingebunden. Das Registrieren und Verwalten personenbezogener Daten gehört ebenso dazu wie die Herstellung und Ausgabe der Dokumente. Um sichere Identitäten gewährleisten zu können, muss diese gesamte Prozesskette wirkungsvoll vor Missbrauch und Manipulation geschützt werden. Als Hochsicherheitsunternehmen ist die Bundesdruckerei bestens dafür gerüstet: Sie verfügt über langjährige Erfahrung in der Konzeption und Integration digitaler Netzwerkstrukturen. Seit 2007 betreibt die Bundesdruckerei erfolgreich die weltweit größte hoheitliche Public-Key-Infrastruktur (PKI). Auf Wunsch unterstützt sie ihre Kunden schon bei der Definition von Anforderungen an einen neuen Reisepass und baut darauf abgestimmt die gesamte Prozesskette für entsprechende ID-Systeme auf.

Daten erfassen und registrieren

Bevor Ausweisbehörden Reisepässe ausgeben können, müssen sie die Daten des Antragstellers korrekt aufnehmen und sicher an den Passhersteller weiterleiten. Bei diesem sogenannten Enrolment unterstützt sie die Bundesdruckerei mit individuellen Lösungen. Die ID-Enrolment-Plattform etwa enthält mehrere miteinander kombinierbare Bausteine, die sich individuell an die Bedürfnisse des Kunden anpassen lassen. Zur Hardware-Infrastruktur zählen Personal Computer, Server und Lesegeräte zum schnellen Auslesen der Daten auf bereits vorhandenen Identitätsdokumenten. Darüber hinaus liefert die Bundesdruckerei Spezialkameras, mit denen man nach standardisierten Vorgaben Gesichtsbilder fotografiert, Unterschriftenpads zur elektronischen Erfassung von Signaturen sowie verschiedene Arten von Scannern. Diese nehmen zum Beispiel Fingerabdrücke als komprimierte Bilder auf oder lesen Formulare ein. Sind die Daten erfasst, prüft eine spezielle Software ihre Qualität und leitet sie weiter an den Passhersteller. All diese Schritte sichert die Bundesdruckerei durch eine verlässliche und sichere PKI ab. Die erfassten Daten werden digital verschlüsselt und signiert. Ausschließlich Personen und Geräte, die in das System integriert sind, haben Zugriff darauf und können die Daten verarbeiten. So wird gewährleistet, dass in den nächsten Prozessschritten nur echte und authentische Daten verwendet werden. Das elektronische Enrolment der Bundesdruckerei lässt sich unkompliziert in bestehende IT-Landschaften einbinden. Es erfüllt, wie von der ICAO empfohlen, höchste Anforderungen an die Datensicherheit. Bei der Einführung des deutschen ePasses im Jahr 2005 hat die Bundesdruckerei zum Beispiel sämtliche Arbeitsplätze in rund 5.400 deutschen Passbehörden mit der entsprechenden Infrastruktur ausgestattet.

Informationen verarbeiten und übermitteln

Im zweiten Schritt der Prozesskette, der Administration, werden die erfassten Daten verarbeitet und verwaltet. Dafür können, je nach Gesetzeslage und individuellen Vorgaben des Kunden, zentrale oder dezentrale Datenbanklösungen genutzt werden. Bereits die Übermittlung der Daten erfolgt digital codiert, sowohl Text als auch optische Informationen wie Fotos werden in Bits und Bytes umgewandelt und verschlüsselt. Um Zugriff auf die Daten zu erhalten, muss man sich vorab digital authentifizieren und gültige Berechtigungszertifikate vorweisen. Zuständig für das Management solcher Zertifikate sind Zertifizierungsdiensteanbieter wie etwa D-TRUST, das akkreditierte Trustcenter der Bundesdruckerei. D-TRUST errichtet für Kunden überall auf der Welt eigene, maßgeschneiderte Trustcenter und passt seine Zertifizierungsdienste individuell an.

Dokumente entwickeln und herstellen

Für die Produktion von Reisepässen nutzt die Bundesdruckerei modernste Anlagen und das Know-how erfahrener Spezialisten. So ist es möglich, den Kunden eine Kombination diverser Hightech-Verfahren anzubieten und für sie maßgeschneiderte Lösungen zu entwickeln. Die Forschungsabteilung der Bundesdruckerei arbeitet dafür kontinuierlich an neuen Produktionsverfahren und entwickelt Methoden, um innovative Sicherheitsmerkmale in die Reisedokumente zu integrieren. Alle bei der Passherstellung verwendeten Materialien erfüllen höchste Qualitätsanforderungen. Dank der lang-

jährigen Erfahrung in der Herstellung von Reisepässen und anderen Arten von ID-Dokumenten ist die Bundesdruckerei in der Lage, die Produktionsprozesse sehr effizient zu gestalten. Alle Fertigungsstätten sind nach den strengsten internationalen Richtlinien sicherheitszertifiziert und -auditiert. Auch von seinen Lieferanten erwartet das Unternehmen hohe Professionalität: Die Bundesdruckerei kooperiert nur mit Zulieferern, die nachweislich für Qualität bürgen können.

Unikate schaffen und ausgeben

Erst mit den persönlichen Daten des Antragstellers wird ein Reisepass zum Unikat. Die Bundesdruckerei betreibt dafür eines der größten Spezialzentren der Welt. Für die Personalisierung der Dokumente bietet das Unternehmen maßgeschneiderte Lösungen an. Kunden haben die Wahl zwischen einzelnen Komponenten oder kompletten Personalisierungssystemen. Alle Lösungen können sowohl zentral als auch dezentral eingerichtet werden: Beim zentralen Einsatz verwaltet eine einzige, hochsichere Produktionsstätte die Daten. Sie bringt die persönlichen Daten optisch, zum Beispiel mit Laser-Personalisierungsmaschinen, auf das Dokument auf und beschreibt zeitgleich den Chip mit den biografischen oder biometrischen Daten. Wählt der Auftraggeber die dezentrale Variante, erfolgt sowohl die optische als auch die elektrische Personalisierung der Dokumente in mehreren, regionalen Büros des Kunden, die den Pass direkt nach der Beantragung selbst ausstellen. Auch Kombinationen aus zentraler und dezentraler Produktion sind möglich. Seit 2010 liefert die Bundesdruckerei beispielsweise mit Sicherheitsmerkmalen ausgestattete Blankopassbücher nach Zypern, wo sie dann zentral personalisiert und anschließend ausgegeben werden. Die Daten und das Farbfoto des Passinhabers werden per Tintenstrahl auf die Datenseite aufgedruckt. Die beschriebene Datenseite wird anschließend mit einer speziellen Sicherheitsfolie laminiert, die die personenbezogenen Angaben versiegelt und dadurch gegen Veränderung schützt. Die Bundesdruckerei liefert für alle Verfahren hochmoderne Techniken. Neben Highspeed-Personalisierungsmaschinen im Großformat hat die Bundesdruckerei auch kompakte, hochwertige Desktop-Geräte im Angebot. Sie eignen sich vor allem für Behörden und Botschaften kleinerer Länder, die nur eine geringe Menge von Pässen personalisieren. Die Personalisierungslösungen lassen sich unkompliziert an neue Dokumententypen anpassen. Alle von der Bundesdruckerei dafür bereitgestellten Software-Pakete entsprechen internationalen Standards. Damit die ausgebenden Stellen die Dokumente prüfen und ändern können, bietet die Bundesdruckerei außerdem spezielle Lese- und Änderungsterminals an.

Daten prüfen und Reisepässe aushändigen

Bevor Mitarbeiter von Ausweisbehörden den fertigen Reisepass ausgeben, müssen sie prüfen, ob die Daten korrekt hinterlegt sind und der Abholer mit der ausgewiesenen Person identisch ist. Lesegeräte der Bundesdruckerei unterstützen sie dabei. Auch Bürger können die Daten auf der Chipkarte ihres Ausweises lesen und überprüfen, wenn sie das Dokument entgegennehmen. Damit erhalten sie volle Transparenz im Hinblick auf ihre elektronisch gespeicherten Daten. Die Lesegeräte benötigen ein Zertifikat, das über eine Public-Key-Infrastruktur abgefragt wird.

Dokumente prüfen und verifizieren

Um im Umlauf befindliche Reisepässe schnell und sicher prüfen zu können, benötigen Behörden zuverlässige Geräte und Systeme. Die Bundesdruckerei bietet ihren Kunden maßgeschneiderte Lösungen: Verschiedene Lese- und Prüfgeräte sind auf die Bedürfnisse von Behörden abgestimmt – darunter auch mobile Geräte, die sich für den Außeneinsatz auf Schiffen oder auf Streife eignen. Mit der dazugehörigen Software können Grenz-, Zoll- und Polizeibeamte schnell und zuverlässig prüfen, ob Pässe oder Visa unverfälscht sind. So hat die Bundesdruckerei zum Beispiel die Software VISOCORE® Inspect entwickelt. Mit ihr lassen sich Sicherheitsmerkmale wie Muster oder besondere Designelemente auf Reisepässen kontrollieren sowie Beschädigungen an Folien automatisch prüfen. Bei der optischen Prüfung wertet das Programm auch die maschinenlesbare Zone (Machine Readable Zone, MRZ) von Ausweisen aus und vergleicht zum Beispiel Angaben im Pass mit denen in einem Visum. Ein zusätzliches Modul erlaubt es, vorhandene biometrische Merkmale zu kontrollieren. So können etwa Fingerabdrücke auf einem Chip mit denen einer real anwesenden Person verglichen werden. VISOCORE® Inspect eignet sich nicht nur für Identitätskontrollen an Grenzen, sondern auch für die Überprüfung von Ursprungsdokumenten und bei Fahndungsabfragen.

Als umfassende Lösung stellt die Bundesdruckerei ihren hoheitlichen Kunden zudem die VISOCORE® Border Control Platform zur Verfügung. Die Services in diesem Paket sind modular wählbar und lassen sich flexibel anpassen, erweitern sowie zu- oder abschalten. Neben traditionellen Identitätsprüfungen durch Grenzschutzbeamte

an staatlichen Grenzen oder auf Flughäfen ermöglichen die Module auch vollautomatische Verfahren, bei denen der Reisende sein Identitätsdokument über Selbstbedienungsterminals prüfen lassen kann. Durch solche automatisierten Prozesse können Kontrollen effizient und zügig durchgeführt werden. Zudem lassen sich Passagierströme gezielt lenken (vgl. Kapitel 4). Je nach Bedarf werden die Geräte in komplexe Netzwerksysteme eingebunden, die den Zugriff auf zentrale Datenbanken etwa für Visa regeln.

Lösungen für sicheres Identitätsmanagement

Die Bundesdruckerei unterstützt Behörden weltweit dabei, von den Möglichkeiten moderner Reisedokumente zu profitieren. Dafür baut sie ihr Know-how kontinuierlich aus und entwickelt mit ihrer hauseigenen Innovationsabteilung sowie namhaften Kooperationspartnern Lösungen, um die Identität einer Person zweifelsfrei, sicher und schnell festzustellen und gleichzeitig zu schützen. So trägt die Bundesdruckerei maßgeblich dazu bei, dass auch in Zeiten umfassender Mobilität ausschließlich berechtigte Adressaten Einblick in persönliche Daten erhalten und die Abwicklungsprozesse im internationalen Reiseverkehr für alle Beteiligten komfortabel sind.

GLOSSAR

A

Ausweisdokument
Dokument zur Identifikation und > Authentifizierung einer Person; enthält Informationen, die eine Echtheitsprüfung ermöglichen und die Identität des Dokumenteninhabers nachweisen. Ausweise werden ausschließlich von Behörden ausgestellt.

Authentifizierung
Überprüfung und Bestätigung der Identität einer physisch anwesenden Person, die sich zuvor > authentisiert hat.

Authentisierung
Nachweis der eigenen Identität, etwa mithilfe von Wissen (z. B. Eingabe einer Personal Identification Number), Besitz (Vorzeigen eines Ausweises) oder > biometrischen Merkmalen wie etwa > Fingerabdrücken.

B

Barcode
Maschinenlesbare Schrift, die aus verschieden breiten, parallel verlaufenden Strichen (engl. „bars“) besteht; die gespeicherten Daten werden mit Scannern oder Kameras maschinell eingelesen und elektronisch weiterverarbeitet.

Basic Access Control (BAC)
Zugriffsschutz für die auf > ePässen gespeicherten Daten. BAC stellt sicher, dass Zugriff auf die auf dem Chip gespeicherten Daten nur nach der erfolgreichen > Authentisierung eines berechtigten > Lesegeräts erfolgen kann.

Berechtigungszertifikat
Muss nachgewiesen werden, um den Chip eines > ePasses auslesen zu können; ermöglicht den Zugriff auf zuvor festgelegte Datenkategorien.

Biometrie / Biometrisches Merkmal
Vermessung von quantitativen körperlichen Merkmalen, auf deren Basis eine automatisierte Erkennung möglich wird. Wichtige biometrische Merkmale sind z. B. der > Fingerabdruck, die > Iris, das Gesicht und die Unterschrift einer Person.

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Nationale, dem Bundesministerium des Innern (BMI) in Deutschland nachgeordnete Sicherheitsbehörde; zuständig für Fragen zur Sicherheit in der Informationsgesellschaft. Das BSI stellt die > CSCA-Zertifikate der hoheitlichen > PKI-Hierarchie in Deutschland aus. Zudem verantwortet es die Akkreditierung weiterer > Zertifizierungsdiensteanbieter in Deutschland.

C

Certification Authority (CA)
Zertifizierungsstelle, die > digitale Zertifikate vergibt; alternative englische Bezeichnung für > Zertifizierungsdiensteanbieter und > Trustcenter.

Chip Authentication (CA)
Verfahren, bei dem sich der Chip am > Lesegerät > authentisieren muss; ermöglicht es, geklonte Chips zu erkennen.

Country Signing Certification Authority Certificate (CSCA-Zertifikat)
Bestandteil der > Public-Key-Infrastruktur und wesentliches Sicherheitselement in elektronischen Ausweisdokumenten; enthält die Landeskennung der ausstellenden Behörde.

Country Verifying Certification Authority Certificate (CVCA-Zertifikat)
Bestandteil der > Public-Key-Infrastruktur, berechtigt zum Auslesen der auf dem Chip des > ePasses gespeicherten Daten. Die Berechtigung wird vom Chip bei der > Terminal Authentication geprüft; Zugriff erhalten nur hoheitliche Stellen wie Kontroll- und Meldebehörden.

D

Digitales Zertifikat
Digitaler Datensatz, der bestimmte Eigenschaften von Personen oder Objekten bestätigt und dessen Authentizität und Integrität durch > kryptografische Verfahren geprüft werden können.

Document Signer Certificate (DS-Zertifikat)
Bestandteil der > Public-Key-Infrastruktur; damit signiert der offiziell beauftragte Passhersteller die auf dem Chip gespeicherten Daten und bestätigt somit deren Echtheit.

Document Verifier Certificate (DV-Zertifikat)
Bestandteil der > Public-Key-Infrastruktur; berechtigt nationale Terminals – zum Beispiel an Grenzkontrollen – zum Auslesen der auf dem Chip des > ePasses gespeicherten Daten.

D-TRUST
Akkreditierter > Zertifizierungsdiensteanbieter der Bundesdruckerei, der im speziell abgesicherten Wertdruckgebäude der Bundesdruckerei betrieben wird; bietet Unternehmen und Behörden bewährte interoperable Signaturprodukte, Zertifizierungsdienstleistungen und elektronische Notariatsservices.

E

EAC-PKI
> Public-Key-Infrastruktur, mit der die Verteilung von > EAC-Zertifikaten geregelt wird, die zum Auslesen von gespeicherten Fingerabdrücken berechtigen.

EAC-Zertifikat
Muss nachgewiesen werden, um auf die besonders sensiblen > biometrischen Daten im > ePass zugreifen zu können; bislang nur in den Ländern der Europäischen Union verpflichtend.

eGate
Vollautomatisierte Kontrollstation für > ePässe. Ein > Lesegerät liest die auf dem Chip gespeicherten Daten aus und prüft sie auf Echtheit. Zeitgleich können Zusatzkontrollen wie Datenbankabfragen durchgeführt werden.

Enrolment
Erfassung der für Reisedokumente nötigen persönlichen Daten. Die Bundesdruckerei bietet dafür zum Beispiel spezielle Hardware- und Software-Lösungen an, wie > Lesegeräte, Spezialkameras, Unterschriftenpads und verschiedene Arten von Scannern.

ePass / Elektronischer Reisepass
> Reisepass, in den ein kontaktloser >Sicherheits-Chip integriert ist. Darauf sind persönliche Daten und > biometrische Merkmale des Inhabers gespeichert. Gemäß den Anforderungen der > ICAO muss der ePass eine > maschinenlesbare Zone (MRZ) enthalten; als > biometrische Identifizierungsmöglichkeit ist das Gesichtsbild vorgeschrieben.

Extended Access Control (EAC)
Erweiterter Zugriffsschutz für die auf dem Chip von > ePässen gespeicherten Daten, der verschiedene Protokolle bündelt. Dazu gehören etwa die Protokolle der > Chip Authentication.

F

Fingerabdruck-Erkennung
> Biometrisches Identifikationsverfahren, bei dem ein Fingerabdruck-Scanner zuerst das Bild des Fingerabdrucks aufnimmt und anschließend das Bild oder ein > Template des Fingerabdrucks auf dem Chip des > ePasses speichert.

G

Gesichtserkennung
> Biometrisches Identifikationsverfahren, bei dem die Merkmale des Gesichts der zu prüfenden Person mit einem oder mehreren gespeicherten Referenzfotos verglichen werden.

I

ID3
Von der > ICAO vorgegebenes, international gebräuchliches Format für Reisepässe. Es hat die Maße 125 × 88 Millimeter.

ID-System
Zusammenspiel von Hochsicherheitstechnologien (Hard- und Software), das sensible Daten, die elektronisch auf Identitätsdokumenten gespeichert werden, wirksam vor dem Zugriff durch Unbefugte schützt und den Datenaustausch zwischen autorisierten Nutzern managt.

International Civil Aviation Organization (ICAO)
Unterorganisation der Vereinten Nationen; 1944 von 190 Ländern gegründet, um durch multilaterale Regelungen die Luftfahrt zu unterstützen und zu mehr Sicherheit beizutragen. Hat unter anderem das ICAO-Dokument 9303 erarbeitet, das Spezifikationen für maschinenlesbare Reisedokumente enthält. Die Bundesdruckerei ist als einziges Unternehmen der Druckindustrie in der ICAO vertreten. Eine Übersicht über weitere wichtige internationale Gremien und Organisationen ist auf Seite 15 abgebildet.

International Organization for Standardization (ISO)
Internationale Vereinigung nationaler Normungsorganisationen, die Standards für alle Bereiche mit Ausnahme der Elektrik, Elektronik und Telekommunikation erarbeitet.

Iriserkennung
> Biometrisches Identifikationsverfahren, bei dem ein Live-Foto der Augeniris von der zu prüfenden Person erfasst und dann mit dem zuvor gespeicherten Referenzbild verglichen wird.

K

Kontaktbehafteter Chip
Sicherheits-Chip mit sichtbarer Schnittstelle; kann nur bei direktem Kontakt mit einem > Lesegerät ausgelesen werden. Kontaktbehaftete Chips dürfen laut > ICAO nicht für ePässe verwendet werden.

Kontaktloser Chip
Sicherheits-Chip ohne sichtbare Schnittstelle; kann ausgelesen werden, ohne dass mechanischer Kontakt zum > Lesegerät besteht. Die > ICAO erlaubt ausschließlich kontaktlose Chips zur Verwendung in ePässen.

Kryptografie
Sammelbegriff für Verfahren zur Ver- und Entschlüsselung von Informationen. Sie schützen davor, dass Unbefugte auf Daten zugreifen, sie verändern und verfälschen können.

L

Laser-Personalisierungsmaschine
Maschine, mit der die Produzenten von > ePässen wie etwa die Bundesdruckerei die persönlichen Daten optisch auf das polycarbonatbasierte Dokument aufbringen und zeitgleich den Chip mit den biografischen und gegebenenfalls > biometrischen Daten beschreiben können.

Lesegerät
Voraussetzung, um Daten aus Ausweisdokumenten auslesen zu können; muss sich mit einem > Berechtigungszertifikat authentisieren, um Zugriff auf den Chip des Dokuments zu erhalten.

Logical Data Structure (LDS)
Standardisierte, logische Datenstruktur, die eine Reihe obligatorischer und optionaler Datenelemente für die Daten festlegt, die auf den Chips von internationalen Reisedokumenten gespeichert sind.

M

Machine Readable Travel Document (MRTD)
Maschinenlesbares Ausweisdokument, dessen Format von der > ICAO spezifiziert wurde und das mit einer > Maschinenlesbaren Zone ausgestattet ist.

Maschinenlesbare Zone (MRZ)
Sichtbarer Teil eines Ausweisdokuments, der durch optische Texterkennung erfasst werden kann. Die MRZ > ICAO-konformer > Reisepässe enthält in der Regel in standardisierter Form Name, Geburtsdatum und weitere Daten des Dokumenteninhabers sowie Prüfziffern für die Identitätsprüfung.

Masterliste
Signierte Datenstruktur; beinhaltet die > CSCA-Zertifikate aller Nationen, denen ein Land vertraut.

P

Passive Authentisierung (PA)
Prüft die Echtheit und Unverfälschtheit der Daten auf dem > kontaktlosen Chip eines > ePasses. Dafür müssen sie mit einem digitalen > Document-Signing-Zertifikat des Herstellers der Karte signiert sein.

Password Authenticated Connection Establishment (PACE)
> Sicherheitsprotokoll, das den > kontaktlosen Sicherheits-Chip eines elektronischen Identitätsdokuments vor unbefugten Zugriffen schützt. Die > ICAO verwendet dafür den > Begriff Supplemental Access Control (SAC).

Prüfziffer
Einfachste Form einer Prüfsumme, die mit speziellen Verfahren aus einer Vielzahl von Ziffern berechnet wird. Erlaubt es, Fehler bei der manuellen Eingabe von Ziffern zu erkennen; Beispiele sind Ausweisnummern, ISBN oder EAN-Codes.

Public Key Directory (PKD)
Von der > ICAO betriebene Plattform zum Austausch von Signaturzertifikaten sowie > Sperr- und > Masterlisten der teilnehmenden Nationen

Public-Key-Infrastruktur (PKI)
Bezeichnet ein System, das digitale Zertifikate ausstellen, verteilen und prüfen kann.

R

Reisepass
Dokument zur Identifikation und > Authentifizierung einer Person bei Auslandsreisen; enthält Informationen, die eine Echtheitsprüfung ermöglichen und die Identität des Dokumenteninhabers nachweisen. Reisepässe werden ausschließlich von Behörden ausgestellt; internationale Standards und Spezifikationen definiert die > ICAO.

S

Sicherheits-Chip
Berührungslos lesbarer Computerchip, der in > ePässen integriert ist und durch verschiedene > Sicherheitsprotokolle vor dem Zugriff Unbefugter geschützt ist.

Sicherheitsmerkmale
Verschiedene Verfahren und Hightech-Lösungen, die die Fälschungssicherheit von Ausweisdokumenten gewährleisten sollen. Unterschieden werden Substrate, Farben, drucktechnische Anwendungen, haptische und mechanische Anwendungsformen sowie Folien und Overlays. Eine detaillierte Übersicht der Sicherheitsmerkmale, die für ePässe in Frage kommen, findet sich auf Seite 40 ff.

Sicherheitsprotokoll
Festgelegtes Schema von Datenabfolgen für die Kommunikation zwischen einem Chip und einem > Lesegerät. Sicherheitsprotokolle wie > Extended Access Control oder > Password Authenticated Connection Establishment gewährleisten Datenschutz, Fälschungssicherheit und Authentizität der Daten auf dem Chip eines > ePasses.

Sperrliste
Liste aller > CSCA-Zertifikate, die zurückgezogen und damit als ungültig gemeldet wurden; nationale Sperrlisten werden über das > Public Key Directory veröffentlicht.

SPOC (Single Point of Contact)
Technischer Standard, mit dem > EAC-Zertifikate auf europäischer Ebene ausgetauscht werden. Zur Übermittlung der Zertifikate verfügt jede Nation über einen eigenen Server.

Supplemental Access Control (SAC)
Siehe > Password Authenticated Connection Establishment.

T

Template
Datei, die nur die wichtigsten Informationen für die Identifizierung eines zuvor erfassten > biometrischen Merkmals enthält und die daher vergleichsweise wenig Speicherplatz benötigt.

Terminal Authentication
Verfahren, mit dem sich das > Lesegerät beim Chip > authentisieren muss; schützt die auf dem Chip gespeicherten > biometrischen Daten vor unbefugtem Zugriff.

Trustcenter
Akkreditierter > Zertifizierungsdiensteanbieter

Z

Zertifizierungsdiensteanbieter (ZDA)
Englisch: > Certification Authority; Dienstleister, der qualifizierte Zertifikate oder qualifizierte Zeitstempel ausstellen darf. In Deutschland sind ausschließlich akkreditierte ZDA befugt, > Berechtigungszertifikate für hoheitliche Ausweisdokumente wie den > Reisepass auszustellen.

Bundesdruckerei GmbH
Unternehmenskommunikation
Oranienstraße 91
10969 Berlin
www.bundesdruckerei.de

Stand Juli 2013

www.bundesdruckerei.de