EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLO FEDERALE DELLE FINANZE
SWISS FEDERAL AUDIT OFFICE

Parallel Audit Biometrischer Pass

FEDPOL, BBL UND ISC-EJPD

EFK-14381/ inkl. Stellungnahmen / 18. Dezember 2014

Impressum

Bestelladresse **Adresse de commande** **Indirizzo di ordinazione** **Order address**	Eidgenössische Finanzkontrolle (EFK) Monbijoustrasse 45, CH - 3003 Bern http://www.efk.admin.ch
Bestellnummer **Numéro de commande** **Numero di ordinazione** **Order number**	1.14381.403.00133.09
Zusätzliche Informationen **Complément d'informations** **Informazioni complementari** **Additional information**	E-Mail: info@efk.admin.ch Tel. + 41 58 463 11 11
Originaltext **Texte original** **Testo originale** **Original text**	Deutsch Allemand Tedesco German
Zusammenfassung **Résumé** **Riassunto** **Summary**	Deutsch (« Das Wesentliche in Kürze ») Français (« L'essentiel en bref ») Italiano (« L'essenziale in breve ») English (« Key facts »)

Das Wesentliche in Kürze

Im Rahmen der Europäischen Organisation der Obersten Rechnungskontrollbehörden ORKB (EUROSAI) wurde im Vorfeld durch die Arbeitsgruppe IT-Revision die Ausstellung von biometrischen Pässen als Prüfungsgegenstand bestimmt. Die Wahl basierte auf den gemeinsam bestehenden Anforderungen an Pässe mit biometrischen Merkmalen. Die Prüfungen wurden in Form eines internationalen „Parallel Audit" durchgeführt. Die Prüfungsgrundlagen und Prüfprogramme sind mit den sechs teilnehmenden Ländern abgestimmt worden.

Ziel der Revision ist eine Beurteilung der Prozesse und organisatorischen Abläufe über den Lebenszyklus der aktuellsten Generation von Schweizer Pässen mit biometrischen Merkmalen. Die Prüfung deckt die Prozesskette vom Antrag für einen neuen Pass bis zur Auslieferung an den Antragssteller ab. Zur Beurteilung der eingesetzten IKT-Systeme und verwendeten Einrichtungen hat die Eidgenössische Finanzkontrolle (EFK) die grundsätzlichen Anforderungen an generelle IT-Kontrollen (ITGC) zugrunde gelegt. Diese Anforderungen werden bei IT-Prüfungen üblicherweise im Rahmen der schweizerischen Prüfungsstandards angewendet.

Die EFK beurteilt das Ergebnis der durchgeführten Prüfung als gut und betrachtet die Abläufe vom Antrag bis zur Auslieferung des biometrischen Passes als angemessen und kontrolliert. In Bezug auf die eingesetzten Informationssysteme und die verwendeten Installationen erachtet die EFK einige Verbesserungen als notwendig und hat in diesem Bericht entsprechende Empfehlungen abgegeben.

Nachfolgend sind die wichtigsten Feststellungen aufgeführt:

- Für die eingesetzten IT-Anwendungen bestehen Notfallvorsorge- und Ausweichsysteme für Ausfälle und Unterbrüche. Die Notfallmassnahmen haben sich bei Stromausfällen schon bewährt. Ein geplanter, periodischer und ganzheitlicher Test der Notfallmassnahmen wird jedoch nicht durchgeführt.
- Der Bundesrat hat eine neue Rechenzentrumsstrategie für die gesamten IKT-Umgebungen des Bundes definiert. Es ist wichtig, die Passapplikationen in die Planungen für neue Ausweichrechenzentren frühzeitig einzubeziehen.
- Der Bundesrat hat bereits im Jahr 2011 entschieden, vorbereitende Arbeiten für den Aufbau und Betrieb eines zweiten und unabhängigen Produktionsstandortes für die Passherstellung bis spätestens 2016 in Angriff zu nehmen. In naher Zukunft ist zudem eine neue Passgeneration geplant. Die Planung dieser beiden Aktivitäten muss rechtzeitig koordiniert und abgestimmt werden.
- [redacted]

Die vorliegende Berichterstattung erfolgt nur an die schweizerischen Behörden und an die Beteiligten in diesem Prüfprozess. Auf der Ebene der teilnehmenden europäischen Länder wird unter der Leitung der EFK ein anonymisierter Kurzbericht erstellt und gegenseitig ausgetauscht. Er enthält keine Details über allfällig festgestellte Schwachstellen.

L'essentiel en bref

Le groupe de travail Révision informatique de l'Organisation des institutions supérieures de contrôle des finances publiques en Europe (EUROSAI) a préalablement décidé d'examiner les procédures d'établissement des passeports biométriques. Cette décision repose sur les exigences communes que doivent remplir les passeports contenant des données biométriques. Le contrôle a été mené sous la forme d'un audit parallèle au niveau international. Les bases et le programme de l'audit ont été déterminés en concertation avec les six pays participants.

La révision a pour but d'évaluer les processus et l'organisation relatifs au cycle de vie de la dernière génération de passeports biométriques suisses. L'audit couvre l'ensemble du processus, de la demande d'un nouveau passeport à la livraison à son titulaire. Le Contrôle fédéral des finances (CDF) s'est fondé sur les exigences principales des contrôles informatiques généraux (ITGC) pour évaluer les systèmes informatiques et les installations utilisés. Lors des audits informatiques, ces exigences sont en règle générale évaluées d'après les normes d'audit suisses.

Le CDF estime que les résultats de l'audit sont bons et juge le processus de la demande jusqu'à la livraison du passeport biométrique adéquats et maîtrisés. À ses yeux, certaines améliorations s'imposent en ce qui concerne les systèmes informatiques mis en œuvre et les installations utilisées. Le CDF a formulé les recommandations en la matière dans ce rapport.

Les principales constatations sont énumérées ci-dessous :

- Les applications informatiques sont pourvues de dispositifs d'alimentation d'urgence et de systèmes de substitution en cas de panne ou d'interruptions. Les mesures d'urgence se sont révélées efficaces lors de coupures de courant. Toutefois, aucun test planifié de l'ensemble des mesures d'urgence n'est effectué à intervalles réguliers.
- Le Conseil fédéral a défini une nouvelle stratégie en matière de centres de données pour l'ensemble de l'environnement informatique de la Confédération. Il est important de tenir compte suffisamment tôt des applications relatives aux passeports lors des planifications concernant les nouveaux centres de données externes.
- En 2011, le Conseil fédéral a décidé de lancer d'ici 2016 des travaux visant à préparer la mise en place et l'exploitation d'un deuxième centre indépendant de fabrication des passeports. Une nouvelle génération de passeports est en outre prévue dans un avenir proche. La planification de ces deux projets doit être coordonnée et harmonisée en temps utile.
- [redacted]

Le présent rapport n'est destiné qu'aux autorités suisses et aux personnes concernées par l'audit. Le CDF supervisera la rédaction d'un rapport succinct anonymisé avec les pays européens participants. Il sera partagé entre ces derniers et ne comprendra aucun détail sur d'éventuels points faibles.

Texte original en allemand

Audit parallelo sul passaporto biometrico

L'essenziale in breve

Il rilascio di passaporti biometrici come oggetto della valutazione è stato deciso in precedenza dal gruppo di lavoro della revisione IT nel quadro dell'«European Organisation of Supreme Audit Insitutions» (EUROSAI). La decisione si basava sui requisiti comuni applicati ai passaporti con caratteristiche biometriche. Le valutazioni si sono svolte sotto forma di audit parallelo a livello internazionale, mentre le basi e i programmi delle valutazioni sono stati concordati con i sei paesi europei partecipanti.

La revisione si prefigge di valutare i processi e le procedure organizzative relative al ciclo di vita dei passaporti svizzeri biometrici di ultima generazione. L'audit esamina la procedura dalla richiesta di un nuovo passaporto alla consegna al richiedente. Per valutare i sistemi TIC e i dispositivi utilizzati, il Controllo federale delle finanze (CDF) ha definito i requisiti principali per i controlli informatici generali. Di regola, tali requisiti sono applicati ai controlli informatici nell'ambito degli standard svizzeri di revisione.

Il CDF considera buono il risultato della valutazione eseguita, reputa adeguati e verificati il processo dalla richiesta alla consegna del passaporto biometrico. In merito ai sistemi d'informazione impiegati e alle installazioni utilizzate, il CDF ritiene necessari alcuni miglioramenti e nel presente rapporto ha formulato raccomandazioni in merito.

Di seguito le osservazioni più importanti:

- Per le applicazioni IT utilizzate esistono sistemi di emergenza e alternativi in caso di guasti e interruzioni. Le misure d'emergenza si sono rivelate valide nelle interruzioni di corrente. Tuttavia non sarà effettuata una prova pianificata, periodica e complessiva delle misure d'emergenza.
- Il Consiglio federale ha definito una nuova strategia del centro di calcolo per tutti gli ambienti TIC della Confederazione. È importante includere tempestivamente le applicazioni relative ai passaporti nelle pianificazioni dei nuovi centri di calcolo di soccorso.
- Già nel 2011 il Consiglio federale ha deciso di avviare, entro il 2016, i lavori preparatori per istituire un secondo luogo indipendente per la produzione di passaporti. Si sta inoltre studiando un nuovo modello di passaporto. La pianificazione di queste due attività deve essere coordinata per tempo.
- [redacted]

I destinatari del presente rapporto sono unicamente le autorità svizzere e i partecipanti al processo di valutazione. Sotto la direzione del CDF viene redatto un breve rapporto anonimizzato e scambiato con gli stati europei partecipanti. Questo documento non si sofferma sui punti deboli eventualmente individuati.

Testo originale in tedesco

Key facts

Under the aegis of the European Organisation of Supreme Audit Institutions (EUROSAI), the Information Technology Working Group designated the issuing of biometric passports as the subject of the audit in the preliminary stages. The selection was based on the existing joint requirements concerning passports which have biometric features. The audits were conducted in the form of an international parallel audit. The basic principles and the audit programmes were agreed with the six participating countries.

The objective of the audit is to assess the processes and organisational procedures over the life cycle of the latest generation of Swiss passports with biometric features. The audit covers the process from the application for a new passport to delivery to the applicant. As the basis, the Swiss Federal Audit Office (SFAO) used the fundamental requirements for IT general controls (ITGC) to assess the ICT systems and equipment installed. These requirements are usually used in IT audits within the scope of the Swiss auditing standards.

The SFAO considers the result of the audit conducted to be good and regards the process from passport application to delivery of the biometric passport as appropriate and controlled. In relation to the information systems and installations used, the SFAO believes some improvements are necessary and has issued corresponding recommendations in this report.

The main findings are listed below:

- Emergency precaution systems and back-up systems exist for breakdowns and interruptions for the IT applications used. The emergency measures have already proved their worth in the case of power cuts. However, a planned, periodic and comprehensive test of the emergency measures is not carried out.
- The Federal Council has defined a new computer centre strategy for the entire ICT environments of the Confederation. It is important that passport applications are included at an early stage when planning new back-up computer centres.
- The Federal Council decided back in 2011 to start preparatory work on the construction and operation of a second and independent production location for passport production by 2016 at the latest. In addition, a new generation of passports is planned for the near future. The planning of both activities must be coordinated in good time and harmonised.
- [redacted]

This report will be sent only to the Swiss authorities and those involved in this audit. A short, anonymous report will be drawn up and mutually exchanged at the level of the participating European countries, under the leadership of the SFAO. The short report will contain no details about any identified weaknesses.

Original text in German

Inhaltsverzeichnis

1 Auftrag und Vorgehen

1.1 Ausgangslage

Die Eidgenössische Finanzkontrolle (EFK) hat im Frühjahr 2013 anlässlich der Versammlung der IT-Arbeitsgruppe der Europäischen Organisation der Obersten Rechnungskontrollbehörden ORKB (EUROSAI) eine Umfrage durchgeführt. Dabei wurden verschiedene Themen vorgeschlagen, für welche in den teilnehmenden Ländern gemeinsame oder ähnliche Sachfragen vorhanden sind, die im Rahmen einer parallelen Revision geprüft werden könnten.

Die Mehrheit der anwesenden Länder hat sich im Rahmen dieses Treffens für das Prüfgebiet des biometrischen Passes entschieden. Die Hauptgründe für die Wahl waren die gemeinsamen Anforderungen der biometrischen Merkmale in Pässen bei Kontrollen von grenzüberschreitenden Reisen. Die Bestimmungen der biometrischen Merkmale in den Pässen werden durch eine internationale Interessengruppe, in der alle teilnehmenden Länder vertreten sind, abgestimmt. Die EFK hat die Leitung und Koordination dieses „Parallel audit on biometric passports“ übernommen und die Risikoanalyse sowie das Prüfprogramm entwickelt, welches beim Audit in allen Ländern angewendet wurde.

1.2 Prüfungsziel und -fragen

Ziel der Revision war die Prüfung der Abläufe der biometrischen Pässe vom Antrag bis zur Passauslieferung und -beendigung. Zudem wurden die technischen IT-Systeme und Installationen in Form von standardisierten Prüffragen auf der Basis von in der Schweiz verwendeten Prüfungsstandards beurteilt.

Die Prüffragen umfassten die Prozesse um die Bereiche:

- Passantrag
- IKT-Systeme und Datenerfassung für den biometrischen Pass
- Passherstellung
- Passauslieferung
- Passbeendigung

sowie Aspekte aus standardisierten und anerkannten Prüfprogrammen bezüglich der grundsätzlichen Anforderungen an generelle IT-Kontrollen (ITGC) hinsichtlich:

- Entwicklung, Betrieb und Sicherheit der involvierten IKT-Systeme
- Gesetzgebung und Regulationen
- Kosten-/Nutzenmessung
- Personenbezogene Aspekte

1.3 Prüfungsumfang und -grundsätze

Die Prüfung wurde von Hans-Jörg Uwer, Revisionsleiter, und Stéphane Kury im September und Oktober 2014 durchgeführt. Als Basis dienten die von der EFK für alle Länder erstellte Risikoanalyse und das detaillierte Prüfprogramm.

Die Schlussfolgerungen im Bericht stützen sich auf die Analyse der erhaltenen Unterlagen, die Interviews und die Besichtigungen der Produktionseinrichtungen ab.

1.4 Unterlagen und Auskunftserteilung

Die notwendigen Auskünfte erfolgten zuvorkommend, offen und kompetent.

2 Die Besonderheiten eines Parallel Audit

2.1 Das Parallel Audit wird in 6 europäischen Ländern durchgeführt

Folgende Länder nehmen an dieser Parallel-Revision teil:

- Belgien
- Norwegen
- Lettland
- Litauen
- Portugal
- Schweiz

2.2 Die Berichterstattung ist lokal detailliert und international anonymisiert

Die teilnehmenden Länder haben sich darauf geeinigt, dass die detaillierte Berichterstattung nur im Rahmen ihrer lokalen Rapportierung erfolgt.

Für den internationalen Austausch wurde eine zusammenfassende Berichtsvorlage angefertigt, welche die einzelnen Länder der EFK zustellen. Basierend auf diesen Zusammenfassungen wird die EFK eine anonymisierte Ergebnispräsentation in grafischer Form erarbeiten und allen teilnehmenden Ländern verteilen. Die Herkunft der einzelnen konsolidierten Prüfungsresultate ist also nur der EFK bekannt.

Nur die von der Revision betroffenen Verwaltungseinheiten in der Schweiz und die beteiligten Personen erhalten den vorliegenden detaillierten Prüfbericht.

3 Feststellungen betreffend biometrischer Pass bezogener Prozesse

3.1 Der Passantrag kann elektronisch gestellt werden

Ein Passantrag für einen biometrischen Pass kann über das Internet oder im Passbüro direkt gestellt werden.

Für den Passantrag werden persönliche Daten verlangt. Dabei prüft das System, ob diese mit den bereits erfassten Daten übereinstimmen. Abweichungen sind in gewissen Ausnahmefällen möglich. Die Sachbearbeiterin bzw. der Sachbearbeiter im Passbüro prüft beim persönlichen

Termin, ob die Daten gültig und aktuell sind oder ob eine genehmigte Ausnahme vorliegt. Die möglichen Ausnahmen sind in einer Verordnung geregelt.

Der Prozess für die Datenerfassung im Passbüro sieht ein 4-Augen-Prinzip vor. [redacted]

3.2 Die Stammdaten im Pass werden vom Zivilstandsregister übernommen

Die Stammdaten wie Name, Geburtsdatum und weitere Angaben, welche für den biometrischen Pass notwendig sind, werden vom zentralen Zivilstandsregister aus der Datenbank „Infostar" übernommen. Die Daten sind dann ebenfalls in der zentralen Passapplikation gespeichert. Die beantragende Person muss nach Erfassung aller Daten bestätigen, dass die Angaben korrekt sind. Bei Abweichungen können die Daten überschrieben oder geändert werden. Der zuständige Passbearbeiter kontrolliert, ob die geänderten Informationen korrekt angepasst worden sind.

Neben den Stammdaten müssen die biometrischen Daten der beantragenden Person aufgenommen werden. Sie wird fotografiert und muss ihre Fingerabdrücke erfassen lassen.

Für die Erfassung der Fingerabdrücke verlangt das System einen minimalen Qualitätsstandard, den sogenannten „NIST"-Wert. In der Regel wird ein NIST-Wert von 50 verlangt. In Spezialfällen wie z.B. bei abgewetzten Fingerkuppen, genügt auch ein NIST-Wert von 25. Ein Wert von 25 erlaubt zwar noch eine persönliche Einzelidentifikation, genügt jedoch für erweiterte Analysen wie Fingerabdruckvergleiche in Datenbanken nicht.

Nachdem alle Daten erfasst worden sind, bestätigt der Antragssteller mit der erwähnten digitalen Unterschrift die Richtigkeit der Informationen. Im Regelfall kontrolliert eine zweite Person im zuständigen Passbüro im Sinne eines 4-Augen-Prinzips diese Daten nochmals, bevor der Passantrag abgeschlossen wird. Danach erfolgt die weitere Verarbeitung vollständig automatisiert. Die Passapplikation erstellt einen Datensatz mit allen Informationen und übermittelt diese über eine Schnittstelle an einen Server, welcher mit der Passproduktionsmaschine verbunden ist. Dann wird die Passproduktion lanciert.

3.3 Die Passherstellung erfolgt zentralisiert und kontrolliert

Nach der Datenerfassung und -übermittlung an die Passproduktion erfolgt die Passherstellung automatisiert an einem zentralen Standort. Ein biometrischer Pass besteht aus verschiedenen Seiten für Sichtvermerke, der Polycarbonat-Karte mit dem aufgenommen Foto und den Grunddaten, einem Chip und dem Umschlag.

Nach der Zusammensetzung der Seiten für Sichtvermerke mit Spezialpapier wird der Pass in der Konfektionierungsmaschine zusammengenäht. Im folgenden Schritt kommen die Pässe in eine Personalisierungsmaschine, welche die biometrischen Daten auf den Chip speichert und die sichtbaren Informationen auf die Polycarbonatkarte auflasert. Der Chip ist zusätzlich mit einer digitalen Signatur versehen. Diese gewährleistet den Nachweis der Chippersonalisierung durch eine offizielle Stelle. Nach der Chippersonalisierung können die Daten nicht mehr verändert werden.

Anschliessend erfolgt eine Qualitätskontrolle über das Auslesen der auf dem Chip gespeicherten Daten und zusätzlich durch eine visuelle Kontrolle des gesamten Passes.

[redacted]

Für die Lagerhaltung der Materialien besteht ein detailliertes Inventar. Bestellungen, Anlieferungen und Verbräuche sind im SAP-System für jeden einzelnen Bestandteil präzise vermerkt. Verantwortliche Personen der Passproduktion des BBL kontrollieren zusätzlich einmal jährlich das vorhandene Inventar an Einzelteilen.

Nur für die Passproduktion zuständige Personen besitzen eine Zutrittsberechtigung zu den Lager- und den Produktionsräumen. Zutritte werden stringent kontrolliert und das Kontrolldispositiv umfasst verschiedene Sicherheitsmassnahmen. So dürfen z. B. keine Handys oder Smartphones mit in die Räumlichkeiten genommen werden und jeder Besucher muss sich ausweisen. Weitere technische Sicherheitsvorkehrungen wie Videoüberwachung, Rauchmelder und technische Überwachungseinrichtungen kontrollieren die Räumlichkeiten mit dem Material für die biometrischen Pässe.

Die EFK erachtet den Ablauf der Passproduktion von der Bestellung bis zur physischen Herstellung als zweckmässig.

3.4 Die Passauslieferung ist vereinheitlicht und nachvollziehbar

Das BBL versendet den biometrischen Pass an die im Passantrag angegebene Versandadresse im Inland eingeschrieben mit der Schweizer Post. Die Passanwendung erstellt beim Druck des Umschlags einen Versandcode, welcher mit der Post koordiniert ist. Nach der Übergabe der Couverts liest die Post den Code ein. Dadurch kann der Versand über die Sendungsverfolgung der Post online überwacht werden. Ausserdem ist bei nicht erhaltenen Pässen der Versandweg nachvollziehbar.

Diplomatenpässe und Pässe mit Auslandadressen in Länder mit langen Versandzeiten der jeweiligen Post werden dem EDA zur Verteilung an die lokale Adresse übergeben.

Mit diesen Massnahmen kann die Zuverlässigkeit der Zustellung in hohem Masse gewährleistet werden. Im abgelaufenen Jahr betrug die Anzahl der verlorenen Pässe im Inland 180 Stück und 56 Stück im Ausland. Die in einer Verordnung festgelegten maximalen Zustellfristen von 10 Tagen im Inland und 30 Tagen im Ausland können eingehalten werden. Reklamationen über nicht erhaltene Pässe sind selten und werden zentral vom fedpol bearbeitet.

3.5 Die Passapplikation kontrolliert die Integrität des Passstatus nicht

Biometrische Pässe haben eine maximal gültige Laufzeit von 10 Jahren. Die Information ist im Pass ersichtlich, im Chip gespeichert und in der Passdatenbank mitgeführt. Die Passapplikation enthält auch die Daten aller früher ausgestellten Pässe mit einem entsprechenden Status wie

„gültig“, „gestohlen“ und weitere Status. Wird ein neuer Pass ausgestellt, sollte der alte Pass keinen gültigen Status in der Datenbank mehr aufweisen, sofern es sich nicht um einen Ausnahmefall handelt. Ausnahmefälle betreffen z. B. Zweitpässe, welche für Reisen in bestimmte Länder notwendig sind. [redacted] Wie viele Fälle insgesamt betroffen sind, kann die EFK aufgrund der Einzelprüfung nicht beurteilen. Weil verschiedene Länder abgelaufene Pässe noch während einer gewissen Zeit als gültiges Ausweisdokument akzeptieren, können diese nicht automatisch nach Ablauf der offiziellen Gültigkeitsdauer inaktiviert werden.

Empfehlung 1 (Priorität 2)

Die EFK empfiehlt, Massnahmen zu analysieren und umzusetzen, welche die Integrität der Daten in der Passanwendung so weit wie möglich sicherstellen und manuelle Erfassungsfehler weitestgehend ausschliessen.

Stellungnahme des fedpol:
fedpol wird dieses Thema im Rahmen der jährlichen Bereinigungsarbeiten zusammen mit den Kantonen und den Schweizer Vertretungen im Ausland angehen. Anhand von entsprechenden Datenbankauswertungen können die beteiligten Behörden aufgefordert werden, allenfalls betroffene Dossiers zu bereinigen.

Das Abhandenkommen eines Passes wird in der Passanwendung und der entsprechenden polizeilichen Datenbank vermerkt. Informationen über gestohlene Pässe werden international mit den entsprechenden Stellen wie Europol oder Interpol koordiniert und ausgetauscht.

4 Feststellungen zu den IKT-Systemen und dem Produktionsumfeld

4.1 Notfallmassnahmen sind nicht systematisch getestet und [redacted]

Für die IKT-Systeme und für die Passproduktion bestehen Notfallvorsorge- und Ausweichmöglichkeiten. [redacted] bei Katastrophen wie atomaren Unfällen oder Grossbränden zu Problemen für die Weiterführung der Passproduktion führen.

Die auf den IKT-Systemen betriebenen Pass-Anwendungen sind in ein umfangreiches Notfall- und Ausweichkonzept eingebunden. Dieses beinhaltet gespiegelte und virtualisierte Umgebungen in zwei getrennten Rechenzentren (RZ). Das Konzept ist in Form eines Business Continuity Management-Projekts (BCM) dokumentiert. Das Funktionieren dieser Ausweichmassnahmen wurde in den letzten Jahren aufgrund von ungeplanten Unterbrüchen bei der Stromversorgung erfolgreich nachgewiesen. Die technischen Systembetreuer führen bisher jedoch keine systematische und periodisch wiederkehrende Tests durch, wie dies nach Realisierung des BCM-Projektes geplant ist. Die EFK erachtet regelmässige Tests von Ausweichmassnahmen als notwendig, um deren Funktionieren im Notfall und beim Eintreten von Katastrophen nachzuweisen.

Empfehlung 2 (Priorität 1)

Die EFK empfiehlt dem ISC-EJPD, definierte Notfallmassnahmen und Ausweichszenarien mindestens einmal jährlich zu testen. Die Tests und die entsprechenden Ergebnisse sind systematisch zu dokumentieren.

Stellungnahme des ISC-EJPD:
Der Umfang und die Periodizität der Tests der Notfallmassnahmen und Ausweichzenarien werden mit dem Anwendungsverantwortlichen fedpol festgelegt und in das ITCSM und BCM aufgenommen.

[redacted]

Die EFK erachtet dies als ideale Ausgangslage, im Rahmen der neuen RZ-Strategie die gesamten Datensicherungen, Ausfall- und Notfallmassnahmen von Passanwendungen bei den entsprechenden Planungen frühzeitig einzubringen.

Empfehlung 3 (Priorität 1)

Die EFK empfiehlt dem ISC-EJPD, im Rahmen der neuen RZ-Strategie des Bundes die gesamte IKT-Umgebung für die Passanwendung in den Planungen rechtzeitig zu berücksichtigen.

Stellungnahme des ISC-EJPD:
Das ISC-EJPD ist sowohl bei der Erarbeitung der RZ-Strategie des Bundes wie auch beim Projekt RZ Campus beteiligt und stellt so sicher, dass die BCM Belange sichergestellt werden.

Die Anlagen, auf welchen die Produktion der Pässe erfolgt, sind alle in den gleichen Räumlichkeiten untergebracht. Es bestehen drei verschiedene Produktionslinien. Diese Installationen stellen sicher, dass bei einem Ausfall von nur einer Anlage die Passproduktion trotzdem erfolgen kann. [redacted]

[redacted]

Der Bundesrat hat diese Schwachstelle erkannt und mittels Beschluss vom 16. Dezember 2011 entschieden, dass eine Passproduktion an zwei räumlich getrennten Standorten geplant werden soll. Ein entsprechendes Projekt muss bis 2018 abgeschlossen sein und vorbereitende Aktivitäten wurden gestartet.

Die nächste Generation von Pässen mit erweiterten Daten und neuen Sicherheitsmerkmalen ist bereits geplant. Dafür müssen in nächster Zeit Ausschreibungen vorbereitet und entsprechende Projekte gestartet werden. Die EFK erachtet es als wichtig, die Arbeiten für den Aufbau eines zusätzlichen Produktionsstandortes und die vorbereitenden Aktivitäten für eine neue Passgeneration zu koordinieren. Der Zeitplan ist, insbesondere für den Aufbau eines zweiten Produktionsstandortes, relativ eng gesetzt und die vorbereitenden Tätigkeiten sind daher möglichst rasch einzuplanen.

Empfehlung 4 (Priorität 1)

Die EFK empfiehlt dem BBL und dem fedpol, die vorbereitenden Arbeiten für den Aufbau eines zweiten Produktionsstandortes und die Aktivitäten für die Planung einer neuen Passgeneration weiter voranzutreiben und eng zu koordinieren.

Stellungnahme des BBL:

Die vorbereitenden Arbeiten für den Aufbau eines zweiten Produktionsstandortes und die Aktivitäten für die Planung einer neuen Passgeneration werden vom BBL und dem fedpol bereits eng in Arbeitsgruppen und dem Projektausschuss koordiniert. Das Projekt wird demgemäss weiter fortgesetzt. [redacted]

Stellungnahme des fedpol:

Die Ausschreibung für die neue Passgeneration erfolgt 2015. Das BBL wird zur Frage des zweiten Produktionsstandorts Stellung nehmen. Die diesbezüglichen Arbeiten werden im Rahmen der Projektarbeiten zwischen BBL und fedpol eng koordiniert.

4.2 Die zentrale Passanwendung wird vom IKT-Leistungserbringer des EJPD betrieben

Die IT-Anwendungen zur Ausstellung von biometrischen Pässen sind vom IT-Leistungserbringer des EJPD, dem ISC-EJPD, entwickelt worden. Das ISC-EJPD ist auch für den sicheren Betrieb der IKT-Umgebung zuständig.

Für Betrieb und Unterhalt der Passapplikationen bestehen Service Level Agreements (SLA) zwischen dem fedpol und dem ISC-EJPD. Diese regeln die vereinbarte Verfügbarkeit, die Zuständigkeiten und die gegenseitige Zusammenarbeit.

Der Change-Management-Prozess für Anpassungen an den Passanwendungen ist standardisiert. Alle Programmänderungen unterliegen schriftlichen Abnahmen der Applikationsverantwortlichen seitens des fedpol. Auch sogenannte Hotfixes, d. h. dringende Programmanpassungen ausserhalb des normalen Ablaufs, werden im Nachhinein schriftlich abgenommen.

Geplante und nicht dringende Änderungen werden in Releases zusammengefasst. Neue Releases werden i. d. R. zweimal jährlich geplant. Das fedpol testet diese umfangreich, bevor sie auf der produktiven Umgebung installiert werden. Die Anwendungsverantwortlichen erstellen zwecks Dokumentation der eingeführten Änderungen sogenannte Release-Notes. Damit können sich die Benutzer vorgängig informieren, welche neuen Anforderungen realisiert werden und welche Anpassungen in der aktuellsten Version enthalten sind.

Zugriffsberechtigungen müssen mit einem standardisierten Formular beantragt werden und die Systemverantwortlichen vergeben die Berechtigungen in der Anwendung.

Die Vorgesetzten bei den zuständigen Passbüros überprüfen jährlich, ob die eingerichteten Berechtigungen noch mit den aktuell zuständigen Personen übereinstimmen. Das Ergebnis dieser Überprüfung wird an die Systemverantwortlichen des fedpol gemeldet.

Die EFK erachtet die Organisation in Bezug auf das Änderungswesen von Programmen und den Prozess der Handhabung von Zugriffsberechtigungen als angemessen.

4.3 Die gesetzlichen Bestimmungen und Vorgaben sind klar

Die rechtlichen Rahmenbedingungen und Vorgaben sind geregelt. Es besteht ein Ausweisgesetz (AwG) für die Verwendung von Pässen mit biometrischen Merkmalen. Verschiedene Verordnungen regeln die detaillierte Handhabung und die Prozesse vom Antrag bis zur Ausstellung solcher Pässe.

Zwischen den involvierten Parteien und Bundesämtern sind interne Regelungen in Form von Service Level Agreements (SLA) getroffen.

Verschiedene Auswertungen, Statistiken und Analysen werden für die Herstellung von Pässen in regelmässigen Abständen erstellt. Das fedpol fasst diese Angaben in einem internen Jahresbericht zusammen und rapportiert sie an zuständige Personen. Für die Kontrolle bestehen teilweise automatisierte Kontrollmeldungen. So melden z. B. die IKT-Systeme, wenn ein Pass nicht ausgestellt wurde.

Die EFK hat anhand von mehreren Interviews festgestellt, dass die Überwachungs- und Kontrollfunktionen des fedpol über die mit der Passherstellung involvierten Parteien wie BBL und ISC-EJPD punktuell erfolgen. Aufgrund der erhaltenen Auswertungen und SLA-Analysen kann sich das fedpol einen Überblick über die Leistungserfüllung der mit der Passproduktion involvierten Leistungserbringer verschaffen. Die Überwachungsrechte sind im AwG, SR 143.1, Artikel 6b geregelt. Das fedpol hat ein Konzept erarbeitet, um den Vollzug von Artikel 6b des AwG sicherzustellen. Als eine der Aktivitäten hat das fedpol im laufenden Jahr beim BBL die Dokumentationen

bezüglich Prozesse, Sicherheit und Qualitätssicherung überprüft. Daraus soll im nächsten Jahr ein Bericht entstehen, der aufzeigt, welche Kontrollmassnahmen in den Folgejahren regelmässig durchzuführen sind. Durchgesetzte und dokumentierte Kontroll- und Überwachungsfunktionen sind aus der Sicht der EFK wichtig, um die Leistungserbringung der involvierten Partner standardisiert messen und beurteilen zu können.

Empfehlung 5 (Priorität 2)

Die EFK empfiehlt, im Sinne von durchgesetzten Kontroll- und Überwachungsfunktionen das Konzept für den Vollzug von Artikel 6b des Ausweisgesetzes vollumfänglich umzusetzen.

Stellungnahme des fedpol: fedpol wird das Konzept umzusetzen.

4.4 Das Kosten-/Nutzenverhältnis wird gemessen und ist ausgeglichen

Das fedpol erstellt Kosten-/Ertragsübersichten, um die angeordnete Kostenneutralität zu messen. Dabei werden auch die Ausschusszahlen von Passfehlproduktionen analysiert. Diese betragen aktuell ca. 2,4 % aufgrund von Produktionsfehlern und 2 % wegen fehlerhafter Personalisierungen wie z. B. unscharfes Foto. Die Bürgerinnen oder Bürger können ihr Foto bei der Erstellung am Bildschirm anschauen, bevor sie ihr Einverständnis erteilen. Es kommen jedoch immer wieder Fälle vor, wo die Passinhaberinnen oder Passinhaber mit der Fotoqualität nach dem Erhalt des Passes nicht zufrieden sind. Die Möglichkeit besteht auch, bei der Beantragung eines Passes ein eigenes Foto zu verwenden, welches nicht älter als 6 Monate sein darf. 99,9% der verwendeten Fotos werden in der Erfassungskabine im Passbüro erstellt.

Zusammenfassend betrachtet ist die Passproduktion kostendeckend, jedoch subventionieren die normalen Pässe mit Versand im Inland, jene der Auslandschweizer. Im Ausland leben ca. 700‘000 Schweizer Bürger. Diese können irgendwo in einem Konsulat die biometrischen Daten erfassen lassen. Bei einer kostendeckenden Verrechnung müssten Auslandschweizer ca. CHF 600.-- für einen Pass bezahlen. Dies rührt von der kleineren Anzahl Pässe bei ähnlichen Fixkosten her.

Einige Passbüros erstellen Kundenzufriedenheitsumfragen. Diese ergeben praktisch immer positive Werte, vor allem seit der Passantrag über das Internet erfasst wird und online ein Termin gebucht werden kann. Dadurch können die Schweizer Bürgerinnen und Bürger innerhalb von nur 15 Minuten die biometrischen Daten auf dem Passbüro erfassen. Meistens erhält dann der Kunde im Inland den Pass innerhalb von 3 Tagen zugestellt. Das ist ein internationaler Spitzenwert.

Die Entwicklung der Passanwendung oder einer neuen Passgeneration wird über Projekte geführt. Die Kosten bzw. Zeitaufwendungen für die Mitwirkung in den Projekten werden erfasst, jedoch nur für diejenigen Personen, welche hauptsächlich in den Projekten involviert sind. Einzelne zeitliche Aufwendungen von Führungspersonen, welche nur periodisch im Projektvorgehen involviert sind, werden nicht erfasst. Gesamthaft betrachtet konnte das Projekt zur Entwicklung des biometrischen Passes innerhalb der geplanten Aufwendungen abgeschlossen werden.

Die EFK erachtet es als sinnvoll, die Kosten für Entwicklung und Betrieb von zukünftigen Pass-generationen in Form einer Projektbuchhaltung weiterhin detailliert zu messen und nachzuweisen.

Dabei sind die zeitlichen Aufwendungen aller Personen zu rapportieren, welche in den Projekten involviert sind.

4.5 Einem Know-how-Verlust bei Personalfluktuationen ist vorzubeugen

Die mit der Passanwendung und der Herstellung beauftragten Mitarbeiterinnen und Mitarbeiter des fedpol, des ISC-EJPD und des BBL besitzen mittlerweile eine grosse Erfahrung und das Know-how ist auf verschiedene Schlüsselpersonen verteilt.

In der Software-Wartung beim ISC-EJPD sind auch externe Personen involviert. Aktuell ist der Anteil an Externen in diesem Umfeld kleiner als 20 %. Das ISC-EJPD will die Wartung der ISA-Applikation vermehrt auf internes Personal verlagern. Während der Basisentwicklung der Anwendung war der Anteil an externen Entwicklern noch wesentlich höher als 20 %.

Die EFK erachtet die Passproduktion als eine Kernkompetenz der Schweiz. Aus Sicht der EFK sind daher Entwicklung und Betrieb der IT-Anwendungen soweit wie möglich mit bei der Bundesverwaltung angestellten Personen durchzuführen.

[redacted]

5 Schlussbesprechung

Die Schlussbesprechung fand am 5. Dezember 2014 statt. An der Besprechung nahmen teil:

FEDPOL	[redacted]
BBL	[redacted]
ISC-EJPD	[redacted]
EFK	Herr Roland Bosshard, Leiter Fachbereich IT- und Projektprüfungen 2 Herr Hans-Jörg Uwer, Revisionsleiter

Sie ergab Übereinstimmung mit den im Bericht aufgeführten Feststellungen, Schlussfolgerungen und Empfehlungen. Die EFK dankt für die gewährte Unterstützung und erinnert daran, dass die Überwachung der Empfehlungsumsetzung den Amtsleitungen bzw. den Generalsekretariaten obliegt.

EIDGENÖSSISCHE FINANZKONTROLLE

Anhang 1: Rechtsgrundlagen und Glossar

Rechtsgrundlagen Schweiz:

Finanzkontrollgesetz (FKG, SR 614.0)

Ausweisgesetz (AwG, SR 143.1)

Ausweisverordnung (VAwG, SR 143.11)

Verordnung des EJPD über die Ausweise für Schweizer Staatsangehörige (SR 143.111)

Organisationsverordnung für das Eidgenössische Justiz- und Polizeidepartement (OV-EJPD, SR 172.213.1)

Rechtsgrundlagen International:

Europäisches Übereinkommen über die Regelung des Personenverkehrs zwischen den Mitgliedstaaten des Europarates (No 0.142.103)

COUNCIL REGULATION on standards for security features and biometrics in passports and travel documents (No 2252/2004)

Anhang 2: Abkürzungen, Priorisierung der Empfehlungen der EFK

Abkürzungen:

ALK	Arbeitslosenkasse
BBL	Bundesamt für Bauten und Logistik
BCM	Business Continuity Management
EFK	Eidgenössische Finanzkontrolle
EJPD	Eidgenössisches Justiz- und Polizeidepartement
EUROSAI	Europäische Organisation der obersten Rechnungskontrollbehörden OERKB
Fedpol	Eidgenössische Bundespolizei
IKS	Internes Kontrollsystem
IKT	Informations- und Kommunikationstechnologie
ISC-EJPD	Information Service Center des EJPD
ISDS	Informationssicherheit- und Datenschutz(-Konzept)
IT	Informationstechnik
QM	Qualitätsmanagement
QS	Qualitätssicherung
RM	Risikomanagement
RZ	Rechenzentrum
SAP	Firma SAP (Schweiz) AG
SLA	Service Level Agreement

Priorisierung der Empfehlungen der EFK:

Aus der Sicht des Prüfauftrages beurteilt die EFK die Wesentlichkeit der Empfehlungen und Bemerkungen nach Prioritäten (1 = hoch, 2 = mittel, 3 = klein). Sowohl der Faktor Risiko [z. B. Höhe der finanziellen Auswirkung bzw. Bedeutung der Feststellung; Wahrscheinlichkeit eines Schadeneintrittes; Häufigkeit des Mangels (Einzelfall, mehrere Fälle, generell) und Wiederholungen; usw.], als auch der Faktor Dringlichkeit der Umsetzung (kurzfristig, mittelfristig, langfristig) werden berücksichtigt. Dabei bezieht sich die Bewertung auf den konkreten Prüfgegenstand (relativ) und nicht auf die Relevanz für die Bundesverwaltung insgesamt (absolut).