Parallel Audit on Biometric Passports

EUROSAI @ IT Working Group

Consolidated Report for the participating SAIs

Management Summary

The evaluation of the reported results showed that the overall passport process is generally under control while a couple of high-risk findings were identified in the non-process-specific assessments. In the non-process-specific assessments, most of the countries found deficiencies and weaknesses related to the IS/IT system and the IT management. Medium risks have been identified in the area of laws and regulations, cost-benefit realisation and transparency, as well as in security regulations relating to internal and external personnel.

Table of Contents

Management Summary 2

1. Introduction 4

1.1. Background 4

1.2. Subject area 4

2. Objective and scope of the audit 5

2.1. Audit objective 5

2.2. Key risk areas 5

2.3. Audit scope 6

3. Overview of results 7

3.1. Detailed results per Domain 8

4. Methodology: Lessons Learned 11

5. Appendix – Priorities 12

1. Introduction

1.1. Background

As countries have the same duties concerning biometric passport issuance and have to comply with the same ICAO requirements, the execution of a parallel audit of the biometric passport management process seemed sensible.

Therefore, at the 8th Meeting of the EUROSAI IT Working Group (ITWG), held in Paris, France, in 2013, the Swiss Federal Audit Office (SFAO) agreed to take the lead for a Parallel Audit on Biometric Passports to be carried out in 2014.

Having outlined the major aspects relating to the audit project, the SFAO assumed the organisation and coordination as well as the elaboration of the detailed Common Programme for this parallel audit.

The following Supreme Audit
Institutions (SAI) confirmed their participation:

- Belgium
- Latvia
- Lithuania
- Norway
- Portugal
- Switzerland

Note: For confidentiality reasons the sequence of the above-mentioned countries does not reflect the sequence of the results stated below.

1.2. Subject area

A biometric passport (or ePassport) contains biometric information which serves to authenticate the identity of travellers. Biometric passport management is the process of establishing and implementing the regulation on standards for security features and biometrics in passports and travel documents issued by the member states. The aim is to develop and maintain efficient and secure biometric passport production procedures.

The complexity of the biometric passport process has encouraged many countries to develop (or acquire) computerised information system(s) accompanied by a set of controls. These controls ensure that transactions are recorded accurately and in a timely manner and that transmission channels are secured.

Although member states are bound by the European Regulation on Biometric Passports, there remains the need for national provisions, particularly concerning the issuance procedures and the authority to read and match the data. Moreover, essential questions (e.g. the problem of nation-wide databases) are not addressed by the Regulation and thus left to the member states.

The biometric passport production process includes a combination of software, hardware, people and communication systems that enable and support data input, processing, storage and the issuing of the documents. Biometric passport production is thus dependent on information systems to ensure that states can produce reliable products.

2. Objective and scope of the audit

2.1. Audit objective

The objective of the audit was to assess whether adequate management and control processes are in place relating to the biometric passport production process. Within the primary objective, auditors were expected to ascertain whether the process to obtain a reliable and secure biometric passport is well defined and properly implemented.

The main goal of this audit was to validate the following areas with regard to the production process, including the risk mitigation aspect:

- Benefit realisation
- Security
- Effectiveness and efficiency

The central control objectives and questions to clarify were as follows:

- Is IT aligned with the business (i.e. strategic direction for IT provides stakeholder value)?
- Does IT enable the business and maximise benefits (cost optimisation, innovation, risk reduction)?
- Are IT resources used securely and responsibly?
- Are IT-related risks managed appropriately?

2.2. Key risk areas

The key risk areas include but are not limited to:

- Loss/theft of physical assets and/or electronic information
- Misuse of confidential information
- Non-cost-effective process and procedures (financial risk)
- Reputation risk
- Compliance risk (failing to meet legal and regulatory requirements)
- Sourcing risk

Each participating country was free to decide how the audit should be performed and what exact audit criteria and methods from the Common Audit Programme should be applied.

2.3. Audit scope

The scope of the Parallel Audit on Biometric Passports was to review the full process of application, creation and distribution of the passports, and the storage of confidential data. On a high level, the audit was divided into 'Passport process assessment' and 'Non-process-specific assessment'. While the first part focused more on the process itself, the second part covered the underlying requirements (e.g. information systems/technology/management, laws and regulation, cost benefit and personnel).

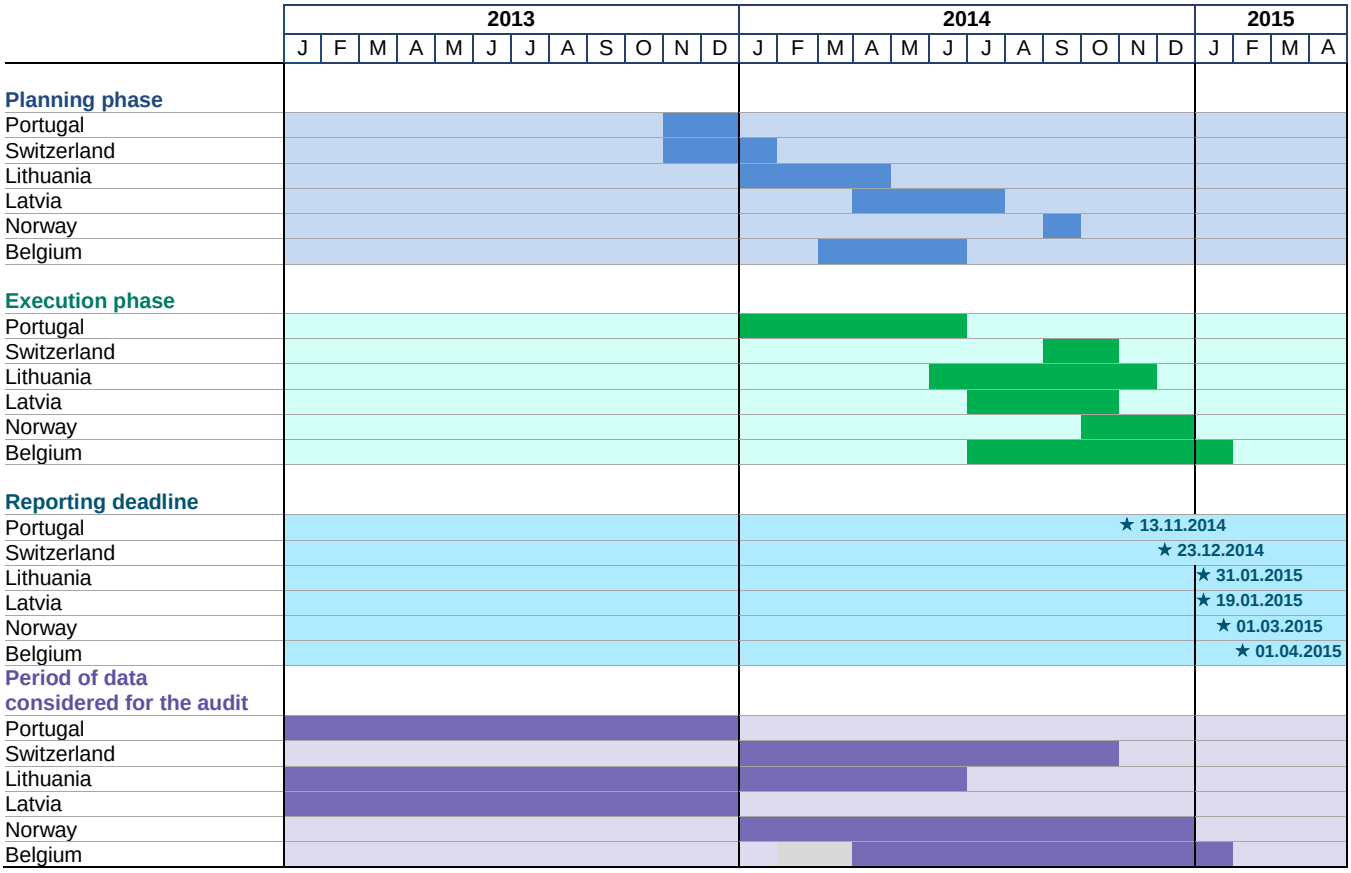
The review of specific data privacy requirements and adherence to technical biometric security standards were not covered by the scope of the Parallel Audit on Biometric Passports.

Based on discussions during a workshop held in Paris, the decision was taken to perform this audit according to the COBIT 4.1 framework, where applicable. Furthermore, the following underlying frameworks were used to design the Common Audit Programme:

- ISO 27002
- ICAO - International Civil Aviation Organization (Doc. 2909)

The Parallel Audit on Biometric Passport production was performed by the participating countries in four different phases and according to the following timetable:

1. Planning phase
2. Execution phase
3. Reporting deadline
4. Period of data considered for the audit



3. Overview of results

Country	A. Passport process assessment					B. Non-process specific assessment			
	1. Initial passport request	2. Application/ data collection	3. Passport production	4. Passport delivery	5. Passport termination	1. IS/IT/IM	2. Laws and regulations	3. Cost benefit	4. Personnel
1									
2									
3									
4									
5									
6									

Note: for detailed explanations please refer to appendix priorities

Risk categories findings and weaknesses:

- Low (i.e. no control deficits)
- Medium
- High
- Significant aspects not covered in the biometric passport audit (not relevant/out of scope)

Area not completed/Follow-up or open questions (indicate no. of areas open)

3.1. Detailed results per Domain

A. Passport process assessment		
1.	**Initial passport request**	Requester initiates process for new passport (new, expired, lost, etc.) or for a change in the current passport (marriage, child, etc.). Initial phase lasts until the request for passport production has been approved (prior gathering of biometrical data).
2.	**Application/data collection**	Identity identification, authentication and validation, gathering of personal and biometrical data, preparation of passport template, gathered data (preparation and consolidation). Data collection would usually be done in person at a pre-defined location but could also be done by letter.
3.	**Passport production**	Integrity of passport information, passport customising and assembly, quality assurance, handling of production errors.
4.	**Passport delivery**	Delivery of final (created or changed) passport to requester. This can be by post (return receipt) or personal pickup at a counter.
5.	**Passport termination**	Revocation of passports, marking passports invalid, destruction of passports, re-use of lost passports.

B. Non-process specific assessment		
1.	Information Systems (IS)/information technology (IT)/information management (IM)	All IS/IT infrastructure processes and controls ensuring that data storage/backup, access and data transfer are handled properly at any time during the passport-relevant processes.
2.	Laws and regulations	Ensure that procedures within the passport production process, IS/IT as well as using external service providers and outsourcing comply with legal and regulatory requirements.
3.	Cost benefit	Ensure that the passport production process (including operations, governance, security, IS/IT) is cost-effective and that costs are covered by fees.
4.	Personnel	Ensure that employees, contractors and third party users understand their responsibilities and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.

Note: for detailed explanations please refer to appendix priorities

Risk categories findings and weaknesses:

- ● Low (i.e. no control deficits)
- ■ Medium
- ▲ High
- ◆ Significant aspects not covered in the Biometric Passport audit (not relevant/out of scope)
- **/1** Area not completed/Follow-up or open questions (indicate no. of areas open)

A. Passport process assessment		1	2	3	4	5	6
1.	Initial passport request						
1.1.	Authorization	●	■	●	●	●	■
1.2.	Quality (changes to passports)	●	●	●	●	●	■
1.3.	Exceptions	■	◆	●	●	●	■
2.	Application/data collection						
2.1.	Authorization (Wrong person is identified and receives passport)	●	▲	●	■	●	■
2.2.	Authorization (Misuse of data)	●	▲	●	●	●	■
2.3.	Quality (Personal data is not accurate)	●	■	●	●	●	■
2.4.	Quality (Gathered data does not meet requirements)	●	■	●	■	●	■
2.5.	Completeness	●	●	●	●	●	◆
2.6.	Exceptions	●	◆	●	●	●	◆
3.	Passport production						
3.1.	Loss prevention and detection	●	◆	●	●	●	●
3.2.	Completeness	●	◆	●	●	●	●
3.3.	Quality	●	◆	●	●	●	●
3.4.	Authorization (Not authorised passports are produced and misused)	●	◆	●	●	●	●
3.5.	Authorization (Multiple passports (prints) are produced and misused)	●	◆	●	●	●	●
3.6.	Privacy	●	◆	●	●	●	●
3.7.	Exceptions	●	◆	●	●	●	●
4.	Passport delivery						
4.1.	Loss prevention and detection	■	▲	●	■	●	■
4.2.	Authorization	●	▲	●	■	●	◆
4.3.	Exceptions	●	◆	●	●	●	◆
5.	Passport termination						
5.1.	Authorization (Invalid or cancelled passports are not correctly revoked and thus misused)	●	■	●	■	●	●
5.2.	Completeness	■	■	●	●	●	●
5.3.	Authorization (Passports initially reported lost are re-used after retrieval)	●	■	■	■	●	●

B. Non-process specific assessment		1	2	3	4	5	
1.	IS/IT/IM						
1.1.	Organization	●	▲	■	●	●	●
1.2.	Policies, Standards and Procedures	●	▲	▲	■	●	●
1.3.	Third party management	●	■	■	●	●	●
1.4.	Change Management	●	◆	■	■	●	●
1.5.	Risk Management	●	▲	■	●	●	●
1.6.	Vulnerability Management	●	▲	●	■	●	●
1.7.	Identity and Access Management	●	▲	●	■	●	●
1.8.	Security Incident Monitoring	●	▲	●	■	■	●
1.9.	Virus and Malware detection	●	◆	●	■	●	●
1.10.	Communication Security	●	◆	●	●	■	●
1.11.	Information Classification	●	◆	■	●	●	●
1.12.	Physical & environmental security	▲	▲	●	■	●	●
1.13.	Availability Management (incl. Backup)	▲	■	▲	■	■	●
1.14.	Prevention and detection of data confidentiality breaches	●	▲	●	■	●	●
2.	Laws and regulations						
2.1.	Compliance	●	▲	■	■	●	●
2.2.	Third parties	■	■	●	●	●	■
3.	Cost Benefit						
3.1.	Benefit Realization	●	■	■	■	●	■
3.2.	Cost transparency and cost recovery	●	●	●	■	■	■
3.3.	Performance and cost management	●	◆	●	●	●	●
4.	Personnel (internal & external)						
4.1.	Human Security (Theft, fraud and misuse of passports, resources, blank passports and data)	●	■	●	■	●	◆
4.2.	Human Security (Theft, fraud and misuse of passports, resources, blank passports and data)	●	■	●	■	●	◆

Note: The detailed results and findings per domain and country will not be shared.

4. Methodology: Lessons Learned

As part of the debriefing exercise, the SFAO performed a short survey amongst the participating countries. This allowed some important lessons to be drawn for future parallel audits:

- **Valuable experience of sharing and learning:** Parallel audits in general facilitate sharing and learning (new) practices. All of the countries thought that their participation in this parallel audit was worthwhile and interesting. Most of them had never been involved in such an audit before and found many benefits in sharing audit procedures as well as the final results.
- **Right approach:** The chosen approach allowed the audit to be performed within the defined scope and provided for relevant findings in the area of biometric passports.
- **Preparatory activities by leading country:** The Common Audit Programme and the Audit Instructions were established by the SFAO. The participating countries appreciated this preparatory work, as it helped to save time as well as resources and provided a common focus.
- **Involvement of participating countries is important:** The definition of risk areas in the Common Audit Programme was perceived as a significant benefit. Additionally, the comparison of results with those of other countries was appreciated. Sharing ideas and fixing audit-specific details during the preparation phase was also recognised as being helpful. Detailed minutes of the working meetings (conference calls) were also considered useful.
- **Different national realities to be covered:** A parallel audit allows a focus on the main audit topics relevant to different countries and the application of a common methodology to different national realities. Some of the countries adapted the Common Audit Programme to cover their local situation and to comply with national procedures, requirement and standards. However, this tailoring was perceived as challenging. In addition, it was felt that there was some lack of practical examples or best practices for evaluating processes.
- **Parallel audit in itself is a challenge:** The participating countries recognised that preparing, planning and performing a parallel audit is more challenging than executing an individual local audit.
- **KPIs would be useful:** With regard to potential improvements, the participating countries suggested developing clear key performance indicators (KPIs). This would contribute to better performance measurements and comparisons.
- **Common assessment criteria:** In addition to the COBIT criteria, further common assessment criteria would be a valuable input in a next parallel audit.
- **Timeliness of communication:** The participating countries would have preferred to share findings, experiences and primary results more systematically during the execution phase and not only towards the end of the audit.
- **Use of current COBIT framework:** Finally, the participating countries also suggested the use of COBIT 5 for future parallel audits instead of the previous 4.1 version.

In summary, the participating countries perceived this parallel audit as a very rewarding exercise. Implementing these lessons learned in future parallel audits will improve the overall audit approach and provide better support to audit teams.

5. Appendix – Priorities

High:

- High risk of material process and control deficiencies due to a significant weakness in controls
- Significant influence on attaining the business and organisation targets
- Non-compliance likely to have negative consequences with regard to:
  - regulations, ordinances, legislation
  - internal directives, finances, reputation
  - data privacy and data protection

Medium:

- Medium risk of material process and control deficiencies due to a weakness in controls
- Moderate influence on attaining the business and organisation targets
- Non-compliance unlikely to have negative consequences with regard to:
  - regulations, ordinances, legislation
  - internal directives , finances, reputation
  - data privacy and data protection

Low:

- Other control weaknesses
- Possibility of improving and optimising processes and controls