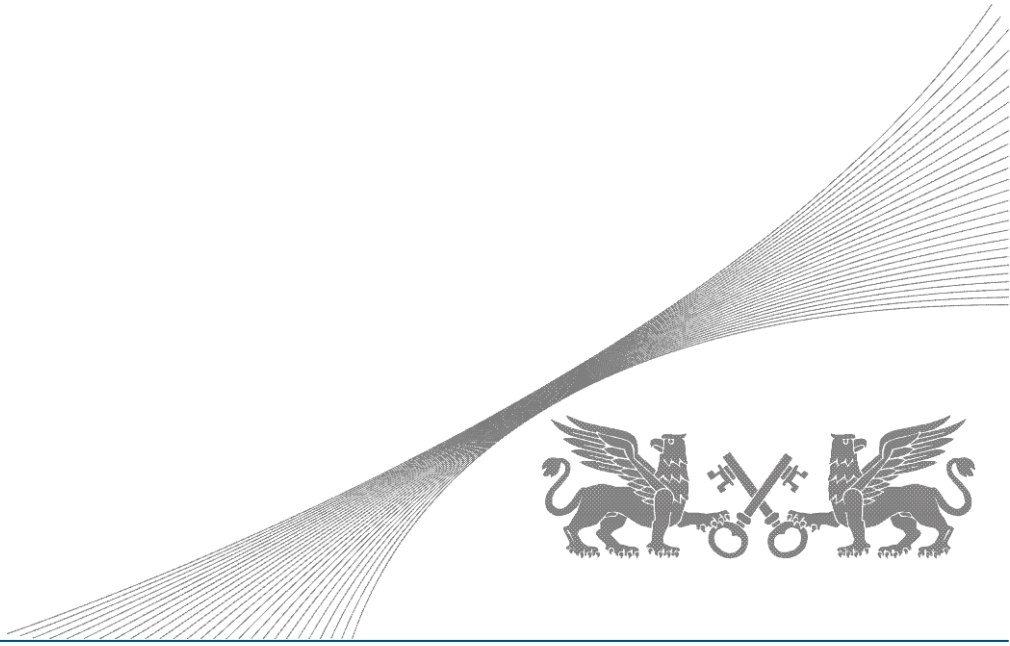
Executive summary of the public audit report

PRODUCTION OF BIOMETRIC DOCUMENTS

27 March 2015 No. VA-P-90-2-6



Full audit report in Lithuanian is available on the website of the National Audit Office: www.vkontrole.lt

www.vkontrole.lt

DEFINITIONS

CIPD refers to the Centre for Issuing Personal Documents under the Ministry of Interior.

SIPD refers to the Information System for Issuing Personal Documents.

SPPD refers to the Information System for Production of Personal Documents.

Authorisation in this report includes not only granting a certain person or program rights to perform certain actions in the data processing system, but also personal identification and acknowledgement, data inspection and confirmation, by comparing records or a record with its reference.

ICAO refers to the International Civil Aviation Organisation, which is an organisation created by the United Nations Organisation, defining international standards, coordinating aviation development, as well as regulating safe and efficient flight areas.

IS refers to information system.

IT refers to information technology.

PKI refers to Public Key Infrastructure, which is an entirety of technical equipment, software, human resources and procedures, used for protection, development management, granting and renewal of certificates, using the methods of public key cryptography.

VPN refers to Virtual Private Network, which means connecting individual remote computer networks into one network using the internet.

EXECUTIVE SUMMARY

Biometric data is used for personal identification, during passenger checking at airports, in the activity of legal institutions, for checking foreign citizens entering the European Union from the third countries, access control and other information systems. For the purpose of facilitating the digital process of personal identification, international standards recommend to supplement personal documents with an integrated electronic microchip, which contains additional personal biometric data (e.g. facial geometry, fingerprints or iris scans, digital photo, etc.). It could also contain additional information, such as an electronic signature. Lithuania issues eight types of personal identification documents with biometric data.

The state policy in the field of issuing personal identification documents is developed by the Ministry of Interior1 and implemented by the Centre for Issuing Personal Documents2. Before 1 February 2015 the Centre has already issued a new generation of 7 047 019 personal identification documents of the Republic of Lithuania. The Residents' Register Service under the Ministry of Justice3, the Police Department, the Migration Department and the Ministry of Foreign Affairs also take part in the implementation of the policy.

The institutions participating in the process of the issue of personal identification documents use a common information system for issuing personal documents SIPD, which operates on the basis of the Residents' Register and thus allows to ensure data reliability and traceability of actions. In 2013 and 2014 the Centre hired a private company for conducting surveillance audits regarding conformity to the ISO/IEC 27001:2005 standards. The auditors did not detect any inconsistencies to the standard requirements and concluded that the information security management system was implemented appropriately and the level of security is good. It is recommended to renew the certification of the information security management system according to the ISO/IEC 27001:2005 requirements. After the evaluation of the process of the issue of biometric personal identification documents, it could be said that there were no substantial shortcomings, except for the already-mentioned details.

The audit of the production of biometric personal identification documents is a part of the international audit, participated by supreme audit institutions from Belgium, Latvia, Lithuania, Norway, Portugal and Switzerland. The goal of the international audit was to evaluate the management and control of the production of personal identification documents. Using the program prepared by the Supreme Audit Institution of Switzerland, we evaluated, whether the document production process in Lithuania is appropriate and ensure that these documents are reliable and secure.

The main subject of the audit was the Ministry of Interior, which develops draft laws in the field of issuing personal documents and supervises the implementation of the state policy in the field of issuing the major personal documents. Audit procedures were conducted at the Centre for Issuing Personal Documents under the Ministry of Interior, which implements the state policy in the field of issuing personal documents, ensures that the design, production and issue of

1 Pt. 9.1 and Pt. 9.8 of the Regulations of the Ministry of Interior of the Republic of Lithuania, approved by the Resolution of the Government of the Republic of Lithuania No. 291 of 14-03-2001 (revision No. 1465 of 13-10-2010).

2 Chapter II of the Regulations of the Centre for Issuing Personal Documents under the Ministry of Interior, approved by the Order of the Minister of Interior of the Republic of Lithuania of 07-02-2011.

3 Chapter II of the Regulations of the Residents' Register Service, approved by the order No. 1R-205 of the Minister of Justice of the Republic of Lithuania. The Regulations approved by the order No. 1V-100 of 07-02-2011 of the Minister of Interior of the Republic of Lithuania were in force until 01-10-2014.

personal documents meets the requirements of the law and international standards; ensures the functioning and development of the public key infrastructure, necessary for recording and checking the biometric personal data into the electronic storage medium of a personal document. The audit covered the period of 2013 and first half of 2014. The information was gathered from the Ministry of Foreign Affairs, the Migration Department under the Ministry of Interior and the Migration Board under Vilnius County Police Headquarters.

The audit did not include a detailed efficiency assessment of biometric document encryption, certificate exchange and applicable cryptographic measures and did not evaluate the compliance of sensitive data to the requirements of classified information processing.

Having evaluated the collected evidence, we provide the conclusions and recommendations of the public report.

CONCLUSIONS

1. Biometric personal identification documents are issued by using the information system for issuing personal documents (SIPD), which was not officially legalised, there are no descriptions of secure procedures and no manager of the system and thus there is no general management equipment maintenance and system development. On the state scale the institutions participating in the process of issuing biometric personal identification documents do not make any assessments, whether the document issue process (operations, security, IS/IT management) is efficient and do not have any data about the costs experienced by other participating institutions (subchapters 2.1 and 2.3).
2. The Centre for Issuing Personal Documents does not keep to some of the requirements defined in the IS/IT management legislation (procedures of IS development, security guarantee or appointment of responsible persons). Up until now this did not have any negative outcome: there were no financial losses or cases of losing data (subchapters 2.1 and 2.2).
3. The shortcomings of the contracts with document issue and software maintenance service providers may influence the process of document issue, because these contracts do not provide any time for troubleshooting or time for maximum recovery of the partial functionality of equipment. Also these contracts do not indicate in what time the service provider should respond to equipment failure, while in case of a critical IT failure the issue of documents would be impossible (subchapters 2.1 and 2.2).
4. There are measures developed for ensuring fluent issue of biometric personal identification documents, also document checking and destruction of lost documents, however:
   4.1. people do not have enough information about the possibility to check biometric documents when receiving their newly-issued personal identification documents;
   4.2. an electronic service for reporting a lost personal identification document enables people to report a lost document at any time of the day. The procedures of reporting lost documents as invalid are implemented only on work days, which creates preconditions for illegal use of personal identification documents (chapter 1.5).

RECOMMENDATIONS

For the Ministry of Interior

1. It is necessary to appoint an administrator for the processes of document issue, who would ensure the resource and cost management of these processes. It would be beneficial to ensure that the equipment used by the institutions participating in the process of the issue of personal identification documents receives appropriate maintenance, while its renewal should be centralised in order to avoid incompatibility (conclusion No. 1).
2. In order to ensure unified development of the information system for issuing personal documents it would be beneficial to define the responsibility of IT management by appointing a system administrator, manager and a data management representative. To legitimise the system by preparing the documents required by the legal acts, which would include fixed scope of the documents managed by the system, connections with other systems/registers and applicable security procedures (conclusions No. 1 and 2).
3. In order to make use of the developed services more efficiently, it would be beneficial to inform people about the opportunity to submit an electronic report about a lost personal identification document and places, where the biometric data could be checked when receiving the newly-made documents (conclusion No. 4).

For the Centre for Issuing Personal Documents under the Ministry of Interior

4. In order to ensure the necessary implementation of security requirements, it would be advisable to implement the missing IT security measures and review the business continuity requirements of the Centre for Issuing Personal Documents (conclusion 2).
5. In order to ensure that the services provided by the third parties meet the demands of the activity: the contracts with the third parties regarding IT services should include conditions, which meet the legal requirements and provisions regarding control and responsibility of service providers (conclusion No. 3).

The measures and terms of the implementation of recommendations are provided in the appendix No. 2.