**AS Sertifitseerimiskeskus**

# Certification service and timestamping service provider's information system audit report

RAS
October 2008
This report contains 7 pages
Appendices comprise 2 pages
Certification service and timestamping service provider information system audit report 2008

# Sisukord

# 1 Summary

## 1.1 The objective of the audit

Our objective is to carry out AS Sertifitseerimiskeskus information systems' audit according to the regulation No. 83 of the Minister of Transport and Communications (October 3, 2000), titled "Auditing procedure of the service providers' information systems". The regulation regulates the auditing process of the certification and time-stamping service provider's (hereinafter SP) information system, with the objective to determine the usability and compliance of the information system with the requirements and norms set by legal acts.

## 1.2 Auditor

The audit was carried out by KPMG Baltics AS *Manager* Janno Kase (CISA certificate nr. 0541738, issued by Information Systems Audit and Management Association on September 15, 2005).

## 1.3 Audit implementation

We carried out the audit between October 1 – October 31, 2008. During the work, we familiarised ourselves with AS Sertifitseerimiskeskus IT environment and documentation, interviewed the key personnel, observed the work processes and carried out other control procedures.

## 1.4 Auditor's decision

We have audited AS Sertifitseerimiskeskus IT environment. We think that the scope of our audit gives sufficient basis for expression of opinion regarding AS Sertifitseerimiskeskus information systems.

We are of the opinion that AS Sertifitseerimiskeskus information system corresponds to requirements provided in the regulation No. 83 of the Minister of Transport and Communications (October 3, 2000), titled "Auditing procedure of the service providers' information systems".

# 2 Evaluations and conclusions

The structure of this part of the report, "Evaluations and conclusions" follows the structure of the regulation No. 83 of the Minister of Transport and Communications (October 3, 2000), titled "Auditing procedure of the service providers' information systems". The regulation has been cited in ***italics and bold***.

## 2.1 High-quality and secure service

***It is checked whether the SP has applied due professional care to guarantee a high-quality and secure service.***

Considering AS Sertifitseerimiskeskus personnel policy, qualifications of employees, thoroughness and conservatism in critical areas, set work methods and existing IT environment, we are of the opinion that the company is capable of guaranteeing certification service and time-stamping service quality and security on a continuous basis.

## 2.2 Compliance with legal acts

***The compliance of the SP information system with «Digital signatures act», «Personal data protection act», «Data bases' act» and the requirements provided by other legal acts and paragraph 16 of this regulation is checked.***

The existing IT environment and planned developments of it do not pose hindrances to guaranteeing compliance of the information system with valid legal acts. AS Sertifitseerimiskeskus information system is compliant with the specified requirements provided in paragraph 16 of the regulation.

## 2.3 Reasons for non-compliance

***Non-compliance with the requirements provided in this paragraph's clause 2*** [in clause 2.2 of this report] ***must be substantiated in the audit report.***

The named non-compliance did not appear during the audit.

## 2.4 Compliance with Certification Practice Statement

***The compliance of the SP information system, including compliance of organisation and work methods, with documented Certification Practice Statement is checked.***

The company's information system, organization and work methods comply with documented Certification Practice Statement to significant extent.

## 2.5 Compliance with Time-Stamping Principles

***The compliance of the SP information system, including compliance of organization and work methods, with documented Time-Stamping Principles is checked.***

The company's information system, organization and work methods comply with documented Time-Stamping Principles.

## 2.6 Fulfillment the requirements of „Digital signatures act"

***Fulfillment of the SP's obligations according to «Digital signatures act» is checked.***

We confirm that AS Sertifitseerimiskeskus complies with the criteria provided in Digital signatures act §18 subsection (1) in clause 1, §25 in clause 1, §19, §21, §26 and §29. AS Sertifitseerimiskeskus is capable of fulfilling the obligations of certification service provider listed in §22 of the act and the obligations of time-stamping service provider listed in §28 of the act. AS Sertifitseerimiskeskus certification practice statement complies with the requirements of Digital signatures act §20. AS Sertifitseerimiskeskus time-stamping principles comply with the requirements of Digital signatures act §27.

## 2.7 EVS-ISO/IEC 12207

***Compliance of the SP's information system is checked against standard EVSISO/IEC 12207, noting in report, which parts of the standard were used for compliance audit.***

We checked compliance with part 6.8 „Problem resolution process" of standard EVS-ISO/IEC 12207. We reached the conclusion that AS Sertifitseerimiskeskus follows principles prescribed in the standard in problem resolution process of certification service and time-stamping service.

## 2.8 EVS-ISO/IEC TR 13335 and ISO/TR 13569

***The compliance of service provider's information system security was checked against standards EVS-ISO/IEC TR 13335-1,2,3 and ISO/TR 13569, noting in report which parts of the standards were used for compliance audit.***

We checked the compliance of the enterprise's information safety management procedure with standard EVS ISO/IEC TR 13335-3 "Guidelines for the management of IT Security. Part 3: Techniques for the management of IT Security" chapter 11 "Follow-up". We reached the conclusion that AS Sertifitseerimiskeskus follows the information security management principles provided in the standard to significant extent.

We checked the compliance of AS Sertifitseerimiskeskus IT environment with part 7.4 „Change control" of standard ISO/TR 13569. We are of the opinion that change management in the software of certification service and time-stamping service AS Sertifitseerimiskeskus follows the requirements provided in the standard.

## 2.9 COBIT

***Compliance of the SP's information system with «COBIT (Control Objectives for Information and Related Technology) Audit guidelines, July 2000, 3 Edition» were checked, noting in the report, which parts of the document were used for compliance audit..***

We checked the compliance of the SP's information system with process DS4 „Ensure continuous service" of COBIT. We came to the conclusion that AS Sertifitseerimiskeskus has followed COBIT's requirements to significant extent.

## 2.10 Specific requirements

***Compliance of the SP's information systems is checked against specific requirements related to certification and time-stamping service provision; note in report, which requirements were used for audit.***

We checked compliance with the requirements stated in part 6 "Obligations and liability" and part 7 "Requirements on CA practice" of the standard ETSI TS 101 456 "Policy requirements for certification authorities issuing qualified certificates" and part 7 "Requirements on TSA practices" of the standard ETSI TS 102 023 "Policy requirements for time-stamping authorities".

We reached the opinion that AS Sertifitseerimiskeskus has followed the good practice provided in the named standards according to expediency proceeding from the size of the company, first and foremost, following the legal acts valid in Estonia.

## 2.11 Other technical norms

***Compliance of the SP's information systems with the technical norms and requirements provided in legal acts significant from the standpoint of provision of service is checked.***

We checked compliance of the company's information security management procedure with part 11 „Business continuity management" of the standard EVS-ISO/IEC 17799:2003. We reached the conclusion that AS Sertifitseerimiskeskus follows the requirements provided in the named standard to significant extent.

At the time the audit was carried out, there were no other significant technical norms and requirements from the standpoint of provision of service set by legal acts.

Yours faithfully

(Report in Estonian signed digitally) (Report in Estonian signed digitally)

Taivo Epner
KPMG Baltics AS Partner

Janno Kase
KPMG Baltics AS Manager, CISA

Annex 1: Confirmation that the audit was carried out during the given period

Annex 2: Copy of CISA certificate of auditor