KPMG
cutting through complexity™

Certification and time-stamping authority audit - audit conclusion

AS Sertifitseerimiskeskus

October 2014

Contents

1 Summary

1.1 The objective of the audit

Our objective is to carry out AS Sertifitseerimiskeskus (hereinafter SK) information systems' audit according to the Regulation No. 68 of the Minister of Economic Affairs and Infrastructure (26 August, 2014), titled "Certification and time-stamping service providers information systems auditing procedure". The regulation governs 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.

Compliance of information system, equipment and procedures were assessed against:

- Digital Signatures Act (8 March, 2000);
- Personal Data Protection Act (15 February, 2007);
- Regulation No. 68 of the Minister of Economic Affairs and Infrastructure (26 August, 2014), titled "Certification and time-stamping service providers information systems auditing procedure";
- ISO/IEC 27001:2005 "Information technology – Security techniques – Information security management systems – Requirements" standard;
- ETSI EN 319 401 "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers supporting Electronic Signatures" v 1.1.1 standard criteria;
- ETSI EN 319 411-2 "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates" v 1.1.1 standard criteria;
- ETSI EN 319 411-3 "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 3: Policy requirements for Certification Authorities issuing public key certificates" v 1.1.1 standard criteria;
- ETSI TS 102 023 "Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities" v 1.2.2 standard criteria.

1.2 Auditor

The audit was carried out by KPMG Baltics OÜ IT auditor Teet Raidma (CISA certificate nr. 0649518, issued by Information Systems Audit and Management Association on September 1, 2006).

1.3 Audit implementation

The audit and all audit procedures were carried out from 15th September – 31st October 2014. During the audit, we familiarized ourselves with SK IT environment and documentation, interviewed SK key personnel, surveyed the work processes and carried out other control procedures.

2 Auditor's decision

We have audited SK IT environment, documentation and key processes.

We think that the scope of our audit and performed operations give sufficient basis for expression of opinion regarding certification and time-stamping services provided by SK.

We are of the opinion that SK information system, controls implemented for certification and time-stamping services comply to significant extent with requirements prescribed in the technical specifications of ETSI and ISO standards, and also with SK Certification Practice Statement and SK Time-stamping Practice Statement. SK services are in accordance with Digital Signatures Act, Personal Data Protection Act and Regulation No. 68 of the Minister of Economic Affairs and Infrastructure (26 August, 2014), titled "Certification and time-stamping service providers information systems auditing procedure".

3 Evaluations and conclusions

The structure of this part of the document "Evaluations and conclusions", follows the structure of §3, section 10) of the regulation No. 68 of the Minister of Economic Affairs and Infrastructure (26 August, 2014). The regulation has been cited in **bold**.

3.1 High-quality and secure service

It is assessed whether the service provider (hereinafter: SP) has applied due professional care to guarantee a high-quality and secure service.

Considering SK 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 and time-stamping services quality and security on a continuous basis.

3.2 Compliance with legal acts

It is assessed whether the SP complies with legal requirements of Digital Signatures Act, Personal Data Protection Act and the requirements of other legal acts.

The existing IT environment and its planned development will not have an impact on the information system in such a way that it would not be able continue ensuring compliance with current legislation.

3.3 Information system and work methods compliance with Certification and Time-Stamping Practice Statement

The compliance of the SP information system, including compliance of organisation and work methods, with documented Certification and Time-Stamping Practice Statement are assessed.

The company's information system, organisation and work methods comply with documented SK Certification Practice Statement and SK Time-Stamping Practice Statement to significant extent.

3.4 Compliance with Digital Signatures Act

It is assessed whether the SP complies with legal requirements of Digital Signatures Act.

We confirm that SK complies with criteria described in the Digital Signatures Act §18 section (1) subsection 1), §25 subsection 1), §19, §21, §26 and §29. SK is capable of fulfilling the obligations of certification service provider listed in §22 and the obligations of time-stamping service provider listed in §28 of the act. SK Certification Practice Statement complies with the requirements of Digital Signatures Act §20 and SK Time-stamping Practice Statement complies with requirements of §27 of the act.

3.5 ETSI EN 319 401, ETSI EN 319 411-2 and ETSI EN 319 411-3

Compliance of the certification service provider and its information system, certification practice statement and security is assessed against standards ETSI EN 319 401, ETSI EN 319 411-2 and ETSI EN 319 411-3 or other comparable publicly approved and available specifications.

We assessed SK's certification service provider information system, its Certification Practice Statement and its security against ETSI EN 319 401, ETSI EN 319 411-2 and ETSI EN 319 411-3

standards. We are of the opinion that SK follows principles prescribed in the standards to significant extent.

3.6 ETSI TS 102 023

Compliance of the time-stamping service provider and its information system is assessed against standard ETSI TS 102 023 or other comparable publicly approved and available specifications.

We assessed SK's time-stamping service provider information system with principles prescribed in standard ETSI TS 102 023. We are of the opinion that that SK follows principles prescribed in the standard to significant extent.

3.7 ISO/IEC 27001:2005

Compliance of the SP's information security is assessed against standard ISO/IEC 27001 or other comparable publicly approved and available specifications.

We assessed SK's information security compliance with standard ISO/IEC 27001:2005. We reached the conclusion that SK follows principles prescribed in the standard to a significant extent in areas of information security.

3.8 Compliance with other technical norms

Compliance of the SP's information system is assessed against technical norms and requirements prescribed in legal acts significant from the standpoint of provision.

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.

Reason for non-compliance

Non-compliance with the requirements provided in this paragraph's section 10 [in section 3.2 of this report] must be substantiated in the audit report.

Non-compliance issues were not identified in the course of the audit.

Yours faithfully

(signed digitally)

Andris Jegers

KPMG Baltics OÜ Partner

(signed digitally)

Teet Raidma

KPMG Baltics OÜ Manager, CISA

Annex 1. Letter of Confirmation

Annex 2. Copy of CISA certificate of auditor

Contact us

Teet Raidma
IT advisory services manager
T +372 6 676 814
E traidma@kpmg.com

www.kpmg.ee