



cutting through complexity™

Time-stamping service audit conclusion

AS Sertifitseerimiskeskus

September 2014



Contents

| | | |
|----------|---|----------|
| 1 | Summary | 3 |
| 1.1 | The objective of the audit | 3 |
| 1.2 | Auditor | 3 |
| 1.3 | Audit implementation | 3 |
| 2 | Auditor's decision | 4 |
| 3 | Evaluations and conclusions | 5 |
| 3.1 | High-quality and secure service | 5 |
| 3.2 | Compliance with legal acts | 5 |
| 3.3 | Reason for non-compliance | 5 |
| 3.4 | Compliance with Digital Signatures Act | 5 |
| 3.5 | SK operations compliance with SK Time-Stamping Practice Statement and SK Practice Statement | 5 |
| 3.6 | ETSI TS 102 023 | 6 |
| 3.7 | EVS-ISO/IEC 12207:1998 | 6 |
| 3.8 | ISO/IEC 13335-3:1999 | 6 |
| 3.9 | ISO/TR 13569:1997 | 6 |
| 3.10 | EVS-ISO/IEC 17779:2003 | 6 |

1 Summary

1.1 The objective of the audit

Our objective of the audit is to assess whether the IS (information systems), apparatus and procedures as implemented by AS Sertifitseerimiskeskus (hereinafter SK) Time-Stamping Service Authority for providing new time-stamping services is in compliance with the following:

- Digital Signatures Act;
- Regulation No. 83 of the Minister of Transport and Communications (October 3, 2000), titled "Auditing procedure of the service providers' information systems";
- ETSI TS 102 023 standard "Electronic Signatures and Infrastructures (ESI);Policy requirements for time-stamping authorities".

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 between July 7th and September 16th 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 AS Sertifitseerimiskeskus 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 new time-stamping services provided by SK.

We are of the opinion that SK information system and time-stamping services comply to significant extent with requirements prescribed in the technical specifications of ETSI TS 102 023 standard and SK Time-Stamping Practice Statement. SK time-stamping services are in accordance with Digital Signatures Act and the regulation No. 83 of the Minister of Transport and Communications (October 3, 2000), titled "Auditing procedure of the service providers' information systems".

3 Evaluations and conclusions

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 time-stamping service 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 other legislation and §16 of regulation No. 83 of the Minister of Transport and Communications (October 3, 2000).

The existing information technology environment and its development will not have an impact on the information system in such a way that it would not be able to ensuring compliance with current legislation. SK information system meets the requirements specified in the §16 of Regulation No. 83 of the Minister of Transport and Communications.

3.3 Reason for non-compliance

Non-compliance issues listed in §2 of Regulation No. 83 of the Minister of Transport and Communications (listed in this report under section 3.2) must be justified in the audit report.

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

3.4 Compliance with Digital Signatures Act

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

We are of the opinion that SK complies with §25 section 1), §26 and §29 of the Digital Signatures Act and is in a position to fulfill the obligations of the listed time-stamping service provider set forth in the §28 of the Digital Signatures Act. SK Time-Stamping Practice Statement meets the requirements set forth in §27 of the Act.

3.5 SK operations compliance with SK Time-Stamping Practice Statement and SK Practice Statement

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

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

3.6 ETSI TS 102 023

Compliance of the SP's information system is assessed against standard ETSI TS 102 023.

We assessed SK's information system compliance with standard ETSI TS 102 023. We have reached to the conclusion that SK follows principles prescribed in the standard in areas of time-stamping authority to significant extent.

3.7 EVS-ISO/IEC 12207:1998

Compliance of the SP's information system is assessed against standard EVS-ISO/IEC 12207, noting in report, which parts of the standard were used for compliance audit.

We assessed compliance with part 5.3 „Development process“ of standard EVS-ISO/IEC 12207. We reached the conclusion that AS Sertifitseerimiskeskus follows principles prescribed in the standard in providing time-stamping services.

3.8 ISO/IEC 13335-3:1999

Compliance of the SP's information system is assessed against standard ISO/IEC 13335-3, noting in report, which parts of the standard were used for compliance audit.

We assessed compliance with part 11.4 „Monitoring“ of standard ISO/IEC 13335-3. We reached the conclusion that AS Sertifitseerimiskeskus follows principles prescribed in the standard in providing time-stamping services.

3.9 ISO/TR 13569:1997

Compliance of the SP's information system is assessed against standard ISO/IEC 13569, noting in report, which parts of the standard were used for compliance audit.

We assessed compliance with part 7.6 „Networks“ of standard ISO/IEC 13569. We reached the conclusion that AS Sertifitseerimiskeskus follows principles prescribed in the standard in providing time-stamping services.

3.10 EVS-ISO/IEC 17779:2003

Compliance of the SP's information system is assessed against standard EVS-ISO/IEC 17779, noting in report, which parts of the standard were used for compliance audit.

We assessed compliance with the requirements stated in part 10 „Systems development and maintenance“ of standard EVS-ISO/IEC 17779. We reached the conclusion that AS Sertifitseerimiskeskus follows principles prescribed in the named standard.

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

(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