Peer Review Services for Assessing Conformity of the Certificate Centre of the State Enterprise Centre of Registers to Standard ETSI TS 101 456 V1.4.3

Audit Report

Audit was conducted by a auditors:

Žydrūnas Skardžius (CISA)

2016

Vilnius

Table of contents

Table 1. Abbreviations and definitions used in the Report

Abbreviation/ definition	Explanation
IT	Information technologies
RCSC	Certificate Centre of the State Enterprise Centre of Registers
CA	Certification Authority of the Certificate Centre of the State Enterprise Centre of Registers
CISA	Certified Information Systems Auditor

1. Introduction

This document is a Peer Review (Audit) Report on Information System of the Certification Authority (hereinafter referred to as the CA) of the Certificate Centre of the State Enterprise Centre of Registers (hereinafter referred to as the RCSC). The audit was conducted to assess conformity of the services provided by the RCSC to the requirements set in Standard ETSI TS 101 456 V1.4.3 (2007-05) “Electronic Signatures and Infrastructures (ESI), Policy Requirements for Certification Authorities Issuing Qualified Certificates”.

Audit was conducted by the service provider experts as follows:

- Žydrūnas Skardžius (CISA);

Audit was conducted in March 2016.

Audit was conducted in communication with the responsible persons at the RCSC and assessing the following documents presented:

- Certification Practice Statement of the RCSC (OID 1.3.6.1.4.1.30903.1.2.3);
- Qualified Certificate Policy of the RCSC (OID 1.3.6.1.4.1.30903.1.1.3);
- Time-Stamping Policy of the RCSC (OID 1.3.6.1.4.1.30903.1.3.1);
- Time-Stamping Practice Statement of the RCSC (OID 1.3.6.1.4.1.30903.1.4.1);
- Statement on Creation and Management of Certificates Created by the Centre of Registers for the Staff of Legal Entities (OID 1.3.6.1.4.1.30903.1.5.1);
- Policy of Qualified Certificates Created by the RCSC for Civil Servants (OID 1.3.6.1.4.1.30903.1.5.1);
- Statement on Creation and Management of Certificates Created by the RCSC for Civil Servants (OID 1.3.6.1.4.1.30903.1.6.1);
- Rules for Electronic Signature approved by Order No v-159 of the Director General of the State Enterprise Centre of Registers as of 31 May 2012;
- Typical Agreement on Provision of Electronic Signature Services;
- Typical Agreement of the State Enterprise Centre of Registers as a Certification Service Provider Rendering Certification Services with the Partner Performing Supporting Certification Services;

As well as assessing public information given on the Internet.

Remark:

When conducting the audit, we assumed that all information and documents provided to the auditors were correct, comprehensive and final, and their copies matched up to the original documents.

Remark:

The conclusions are drawn up on the basis of assessment made by the experts, which largely relied on the information made available to them. Opinion expressed in this Report cannot be regarded as an indisputable legal fact. Assessment made by the experts shall be also considered as the opinion of the experts; therefore it may not coincide with the opinion given by other experts or responsible representatives of the audited party.

2. Audit results

Table 2. Assessment of conformity to Standard LST ETSI TS 101 456 v1.4.3

LST ETSI TS 101 456 v1.4.3 requirements	Conformity to requirements
5 Introduction to qualified certificate policies	-
5.4 Conformance	-
5.4.1 General	Nonconformities identified were not critical
6 Obligations and liability	-
6.1 Certification authority obligations	Nonconformities identified were not critical
6.2 Subscriber obligations	Nonconformities identified were not critical
6.3 Information for Relying parties	No nonconformities identified
6.4 Liability	No nonconformities identified
7 Requirements on CA practice	-
7.1 Certification Practice Statement (CPS)	Nonconformities identified were not critical
7.2 Public key infrastructure - Key management life cycle	-
7.2.1 Certification authority key generation	No nonconformities identified
7.2.2 Certification authority key storage, backup and recovery	No nonconformities identified
7.2.3 Certification authority public key distribution	No nonconformities identified
7.2.4 Key escrow	No nonconformities identified
7.2.5 Certification authority key usage	No nonconformities identified
7.2.6 End of CA key life cycle	No nonconformities identified d
7.2.7 Life cycle management of cryptographic hardware used to sign certificates	No nonconformities identified
7.2.8 CA provided subject key management services	No nonconformities identified
7.2.9 Secure-signature-creation device preparation	No nonconformities identified
7.3 Public key infrastructure - Certificate Management life cycle	-
7.3.1 Subject registration	No nonconformities identified
7.3.2 Certificate renewal, rekey and update	No nonconformities identified
7.3.3 Certificate generation	No nonconformities identified
7.3.4 Dissemination of Terms and Conditions	Nonconformities identified were not critical
7.3.5 Certificate dissemination	No nonconformities identified
7.3.6 Certificate revocation and suspension	No nonconformities identified

LST ETSI TS 101 456 v1.4.3 requirements	Conformity to requirements
7.4 CA management and operation	-
7.4.1 Security management	Nonconformities identified were not critical
7.4.2 Asset classification and management	Nonconformities identified were not critical
7.4.3 Personnel security	No nonconformities identified
7.4.4 Physical and environmental security	No nonconformities identified
7.4.5 Operations management	No nonconformities identified
7.4.6 System Access Management	No nonconformities identified
7.4.7 Trustworthy Systems Deployment and Maintenance	Nonconformities identified were not critical
7.4.8 Business continuity management and incident handling	Nonconformities identified were not critical
7.4.9 CA termination	No nonconformities identified
7.4.10 Compliance with Legal Requirements	No nonconformities identified
7.4.11 Recording of Information Concerning Qualified Certificates	No nonconformities identified
7.5 Organizational	No nonconformities identified

Assessment:

On the whole, requirements of Standard ETSI TS 101 456 V1.4.3 are observed; however some nonconformities, which are not critical, were identified.

A list of such nonconformities and recommendations for their correction are given in the Annex; whereas the CA reaction to the identified nonconformities should follow the procedures described in the Certification Practice Statement of the RCSC.

3. Nonconformities identified/ recommendations

3.1. Nonconformities related to the certificate part "5. Introduction to qualified certificate policies"

5.4.1 General

d) The CA compliance shall be checked on a regular basis and whenever major change is made to the CA operations.

Explanation of requirement	This Point says that audit should be conducted not only on a regular basis but also whenever major change is made.
Description of nonconformity	The Statement says that the CA audit shall be conducted on a regular basis, i.e. every year.
Recommendation	To supplement the CA Certification Practice Statement with a provision that audit shall be also conducted after making a major change.
Nonconformity classification	Nonconformity is not critical

3.2. Nonconformities related to the certificate part "6. Obligations and liability"

6.1 Certification authority obligations

The CA has the responsibility for conformance with the procedures prescribed in this policy, even when the CA functionality is undertaken by sub-contractors.

Explanation of requirement	The CA should ensure that all the requirements and obligations given in Chapter 7 were implemented. The CA shall be responsible for conformance with the requirements, even when the CA functionality is undertaken by sub-contractors.
Description of nonconformity	Agreements do not provide for the sub-contractor auditing procedures; therefore the CA has no possibility to check conformance of the sub-contractor with its obligations.
Recommendation	To review and update typical agreements and introduce an optimal auditing procedure.
Nonconformity classification	Nonconformity is not critical

6.2 Subscriber obligations

g) notify the CA without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the certificate:

i) the subject's private key has been lost (e.g. by forgetting the PIN number needed to use the key), stolen, potentially compromised; or

ii) control over the subject's private key has been lost due to compromise of activation data (e.g. PIN code) or other reasons; and/or

iii) Inaccuracy or changes to the certificate content, as notified to the subscriber or to the subject.

Explanation of requirement	The Standard says that a period of time must be defined during which the subject should notify on the certificate suspension/revocation.
Description of nonconformity	Agreements with the certificate users say that notification should be sent without any reasonable delay in case circumstances stipulating revocation of certificate validity have been identified.
Recommendation	“Without any reasonable delay” should be made concrete. It is recommended to set a maximum period of 12 hours when the subject must notify of the certificate suspension/revocation.
Nonconformity classification	Nonconformity is not critical

3.3. Nonconformities related to the certificate part “7.1 Certification Practice Statement (CPS)”

7.1 Certification practice statement

c) The CA shall make available to subscribers and relying parties its certification practice statement, and other relevant documentation, as necessary to assess conformance to the qualified certificate policy.

Explanation of requirement	All the relying parties must be provided easy access to the Certification Practice Statement or other relevant documents proving conformity to the certification policy.
Description of nonconformity	Agreements with sub-contractors do not have a provision that a sub-contractor should make the Certification Practice Statement of the RCSC or other relevant documents publicly available.
Recommendation	To commit the sub-contractors to add links to the RCSC website (or only to the webpage containing legal information).
Nonconformity classification	Nonconformity is not critical

7.1 Certification practice statement

g) The CA shall define a review process for certification practices including responsibilities for maintaining the certification practice statement.

Explanation of requirement	A review process should be defined and implemented, including also obligation to review the certification practice statement.
Description of nonconformity	Review process is described but it is not properly implemented. The certification practice statement and other related documents are not regularly reviewed; not all review process activities stated are implemented (e.g. planning of tasks after conducting the audit).
Recommendation	• To review and update all relevant documents; • To implement all processes after submission of the Audit Report (i.e. extending beyond the implementation of the recommendations).
Nonconformity classification	Nonconformity is not critical

3.4. Nonconformities related to the certificate part “7.3 Public key infrastructure - Certificate Management life cycle“

7.3.4 Dissemination of Terms and Conditions

b) The information identified in a) above shall be available through a durable (i.e. with integrity over time) means of communication, which may be transmitted electronically, and in readily understandable language.

Explanation of requirement	All the relying parties should be given easy access to the relevant certificate information.
Description of nonconformity	Agreements with sub-contractors do not have a provision that a sub-contractor should make the Certification Practice Statement of the RCSC or other relevant documents publicly available.
Recommendation	To commit the sub-contractors to add links to the RCSC website (or only to the webpage containing legal information).
Nonconformity classification	Nonconformity is not critical

3.5. Nonconformities related to the certificate part “7.4 CA management and operation”

7.4.1 Security management

a) The CA shall carry out a risk assessment to evaluate business risks and determine the necessary security requirements and operational procedures. The risk analysis shall be regularly reviewed and revised if necessary.

Explanation of requirement	The CA must carry out risk assessments to determine the necessary security and operational procedures. Results of a risk assessment must be regularly reviewed.
Description of nonconformity	The risk assessment was not carried out by the RCSC recently.
Recommendation	Risk assessments should be carried out annually or after major changes in the RCSC assets.
Nonconformity classification	Nonconformity is not critical

7.4.1 Security management

b) The CA shall retain responsibility for all aspects of the provision of certification services, even if some functions are outsourced to subcontractors. Responsibilities of third parties shall be clearly defined by the CA and appropriate arrangements made to ensure that third parties are bound to implement any controls required by the CA. The CA shall retain responsibility for the disclosure of relevant practices of all parties.

Explanation of requirement	The CA is responsible for the proper control of all aspects of the provision of certification services, even if some functions are outsourced to third parties. Responsibilities of third parties must be clearly defined and appropriate arrangements made that third parties are bound to implement these responsibilities.
Description of nonconformity	Agreements do not provide for the sub-contractor auditing procedure; therefore the CA has no possibility to check whether the sub-contractor duly executes all the obligations and liabilities imposed.
Recommendation	To review and update typical agreements and to provide for an optimal auditing procedure.
Nonconformity classification	Nonconformity is not critical

7.4.1 Security management

g) CA shall ensure that the security of information shall be maintained when the responsibility for CA functions has been outsourced to another organization or entity.

Explanation of requirement	The CA should ensure security of information even in case a part of the CA functions has been outsourced to third parties.
Description of nonconformity	Agreements do not provide for the sub-contractor auditing procedure; therefore the CA has no possibility to check whether the sub-contractor duly executes all the obligations and liabilities imposed.
Recommendation	To review and update typical agreements and to provide for an optimal auditing procedure.
Nonconformity classification	Nonconformity is not critical

7.4.2 Asset classification and management

a) The CA shall maintain an inventory of all information assets and shall assign a classification for the protection requirements to those assets consistent with the risk analysis.

Explanation of requirement	This Point requires maintenance of an inventory of all information assets, which contains a classification of assets based on the results of risk assessment.
Description of nonconformity	There was a lack of evidence during the audit that the inventory of all information assets has been maintained and is up-to-date.
Recommendation	To prepare and maintain the inventory of all information assets.
Nonconformity classification	Nonconformity is not critical

7.4.7 Trustworthy Systems Deployment and Maintenance

a) An analysis of security requirements shall be carried out at the design and requirements specification stage of any systems development project undertaken by the CA or on behalf of the CA to ensure that security is built into IT systems.

Explanation of requirement	The analysis of security requirements should be carried out at the design and requirements specification stage of the system.
Description of nonconformity	Documentation of the certificate ordering system has not been prepared and is not being maintained.
Recommendation	To document data structures, system functional and non-functional requirements: • We recommend using entity-relationship or class diagrams for data structures. • For documentation of functional requirements – task flow diagrams. • For modelling of system dynamic behaviour – activity, sequence and state diagrams. • For the description of system components – components' diagrams.
Nonconformity classification	Nonconformity is not critical

7.4.8 Business continuity management and incident handling

a) The CA must define and maintain a continuity plan to enact in case of a disaster.

Explanation of requirement	The CA must prepare and maintain a continuity plan, which could be enacted in case of a critical security disaster.
Description of nonconformity	There was a lack of evidence during the audit that a continuity plan of the RCSC has been prepared.
Recommendation	To prepare a continuity plan of the RCSC.
Nonconformity classification	Nonconformity is not critical

4. Audit conclusion

The RCSC audit has been conducted on conformity to the Standard ETSI TS 101 456 V1.4.3 requirements. To our opinion, the scope of audit conducted was enough to prepare the audit conclusion on conformity of the Certification Authority of the RCSC to the requirements set.

General conclusion:

To our opinion, most of the **requirements** imposed by Standard ETSI TS 101 456 V1.4.3 **are implemented;** however some nonconformities or areas to be improved have been identified.

We would like to point out that nonconformities identified, to the opinion of auditors, are not critical; however they should be corrected following the procedure defined in the Certification Practice Statement of the RCSC.