Report on the assessment of
PVIT 018RE -2017

Name and address of the auditee:

NLB d.d.
Republic square 2, 1000 Ljubljana

The type of audit:

Certification of qualified service provider assessment of trust – 2. part – Regulation (EU) No. 910/2014 European Parliament and of the Council of 23 November 1995. July 2014 of electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC of the

Date of assessment: 2017-06-26
Date of report: 2017-06-28

Reviewed By: Approved By:

Mani Mani Jan Jan

SIQ Ljubljana, Tržaška cesta 2,
1000 Ljubljana, Slovenia e-mail:msa@siq.si

The CONTENTS of the

1. INTRODUCTION
2. the FINDINGS of the
2.1. main findings
2.2 non-compliance
2.3 findings and minor non-conformities
3. the CONCLUSION of the

1 INTRODUCTION

Information about the Organization:
The Bank with the mission is much more than the sum of its activities. Its impact on the financial market of NLB with an active role in consolidating all aspects of social development. With the implementation of their business objectives on the basis of tradition and trust and nurturing responsible business values. As the largest Slovenian Bank is aware of the importance of its mission and the fact that the successful development of the company as a whole, reinforcing her reputation and power. NLB certification agency is registered by an authority qualified digital certificates (certificates), which operates in the context of MTS primary responsibility authority qualified digital certificates

certifying the identity of the user, which is similar to the issuing of passports or identity cards, except that a digital certificate in paper form does not exist.

Regulation (EU) No. 910/2014 European Parliament and of the Council of 23 November 1995. July 2014 of electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC has been taken into account in its entirety, without exception.

Legislation and standards:

- The Regulation (EU) No. 910/2014 European Parliament and of the Council of 23 November 1995. July 2014 of electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC of the
- EN 319 401 in 2.1.1 General Policy Requirements for Trust Service Providers
- EN 319 411 Policy and security requirements for Trust Service Providers issuing certificates ● 319 411-1 v1.1.1: General requirements
- 319 411-2 v2.1.1: Requirements for trust service providers issuing qualified certificates to the EU

- EN 319 421 v1.1.1: Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps
- EN 319 412 Certificate Profiles
- 319 412-1 v1.1.1: Overview and common data structures
- 319 412-2 v2.1.1: Certificate profile for certificates issued this natural persons
- 319 412-3 v1.1.1: Certificate profile for certificates issued this legal persons
- 319 412-4 v1.1.1: Certificate profile for web site certificates issued it organisations
- 319 412-5 v2.1.1: QCStatements
- EN 319 422 v1.1.1 Time-stamping protocol and electronic time-stamp profiles

Involve on-site audit methods

Assessment of information security including access queries based on observation and evidence. During the assessment of the appropriate level is determined and representative number of sampling points on the basis of:

- results of internal audits,
- results of the inspection management
- change the size of the cities,
- changes to the business purpose of the individual sites
- the complexity of services
- the complexity of information systems in various locations,
- changes in working practices, ● changes in activities,
- potential interactions with critical information systems or information systems that process sensitive information,
- or sites operated by a subcontractor or other external organisation, ● any regulatory requirements.

Presojevalski plan outlines the key elements of the assessment and annexed to this report.

Presojevalski plan outlines the key elements of the assessment and annexed to this report.

Critical systems

The location of the	Key equipment
Certifikatska agency AC NLB	Identification data (structure) and central servers

Check the documentation

Name of the document
Policy AC NLB Public part of the internal rules of operation 2. Edition of 27.6.2017
Policy AC NLB Confidential part of the internal rules of operation 2. Edition of 27.6.2017
P15-privacy policy analysis of IT risks
The record of generating keys of the root issuer ACNLB v2_V 1.4
Instructions on how to activate a backup system IT
The process of introducing IT to changes in the production environment

The objective of the audit information system is to ensure compliance with the regulation on the electronic identification and trust services for electronic transactions in the internal market (short EIDAS) and of the relevant ETSI standards for the following services:

A digital signature,

Electronic stamp

Electronic time stamp

Electronic delivery is recommended

Certificates for authentication sites

The assessment was conducted in accordance with the schedule attached hereto, are carried out:

● mag, Miha Ozimek, PCI DSS QSA, ASV, CISA, CISM, head of the assessment of the ISO/IEC 27001, ISO/IEC, ISO 20000-1, ISO/IEC 27018 22301, ISO 9001 ● Dr. Andrej Rakar, PCI DSS QSA, ASV

● Andrew Gornik.

Information on the auditor shall

SIQ-Slovenian Institute of quality and Metrology

In the SIQ Ljubljana with its own team of experienced professionals in the field of information security carried out a comprehensive set of security checks, which are adapted according to the needs of each organization. Implement standard security checks (automated inspection of the external and internal vulnerability security checks) and specialized inspection according to the needs of the Subscriber (compliance with the PCI DSS QSA, ASV, and security applications, mobile devices, review compliance with regulation EIDAS, compliance with the regulation, the examination of GDPR source code control systems, SCADA, control of VoIP/IP telephony, social engineering, audit information system).

SIQ is a professional, independent and impartial institution which offers complete solutions in the field of testing and certification of products, management systems assessment, metrology and education.

Their goal is a broad and comprehensive range of support and promote the efforts of organizations to fulfil their objectives for the quality of products and services, and follow their policies to increase productivity and performance. For 50 years cooperate with organisations in accessing the markets, raising productivity, improving the quality and reach of excellence.

International validity and high professional level of their work is also confirmed by a number of accreditations and memberships in international certification schemes and associations. The main competitive advantages of SIQ-have the knowledge and experience of their experts, international visibility and credibility, flexibility, offer integrated solutions and the introduction of new services, and constantly adapting to the market.

m.SC. Andreiu Ozimek

Miha Ozimek is graduated from the Faculty of Security Sciences, University of Maribor, and specialized in the field of information security. He did postgraduate studies in information security in the field of information security standards and deployment policies, the protection of information in an organization, at the Faculty of computer and information science, University of Ljubljana. Runs on the Slovenian Institute of quality and Metrology (SIQ) and quality systems audit and information security in enterprises. During his employment he obtained a certificate for the lead auditor for ISO/IEC 27001, ISO/IEC 20000-1, ISO 22301, ISO/IEC and ISO 9001 27018, also has tested information systems auditor CISA and CISM (head of operations of the verification of information technologies), PCI DSS QSA, ASV.

During the period of one year shall be carried out over 100 internal and external audits in different enterprises (in the field of ICT, health, security and State institutions). Leads and participates in the preparation of projects in connection with the certification of information security management. Educates and prepares the system for ICT sector Auditors (ISO/IEC 27001 and ISO/IEC 20000-1).

He is currently the Vice President of the Slovenian section of ISACA (Silver) and guest lecturer at the Faculty of Security Sciences, University of Maribor, in the field of information protection system.

2 FINDINGS

2.1. main findings

Key audit findings

NLB, d.d. by implementing service AC NLB (organisational and technical) and follow good security practices is sufficient SUVI DO and already partially meets the requirements in accordance with the new regulation on electronic identifikacijah and trust services for electronic transactions in the internal market (shorter, EIDAS-electronic identification and services trust). Employees who participate in the field of information security and services, provide appropriate management of NLB AC AC NLB.

All non-conformities and observations after the certification of qualified service provider assessment of trust-1. part of have been suitably rectified and transmitted to the appropriate answers were shown the modified procedures and documentation, which defines the execution of all the measures necessary to achieve compliance with the EIDAS and the relevant ETSI standards.

During the assessment of the security of the information system, were discovered the lack of conformity, which have been abolished yet over the course of the audit. The dossier, which defines all the activities of the trust service is prepared properly and contains all the controls, which exposes the EIDAS and the relevant ETSI standards.

Was presented to the auditor shall be granted adequate documentation and relevant information with regard to the security policies and procedures. Most of the security controls in accordance with ISO/IEC 27001:2013 standard and represents good practice information security, as described in the ISO/IEC 27002:2013 standard.

All persons who have access to mission-critical information systems are qualified with regard to information security, security policies and an effective system for managing incidents. Every incident in the information system of the CA is detected and properly managed.

2.2 Major non-conformities

During the assessment on the basis of EIDAS and ETSI standards were detected following the non-compliance that have been corrected in the course of the assessment.

1 you will need to supplement chapter limitation of liability (provis. 9.8.)

Conclusion: in section 9.8 of the document Policy AC NLB Public part of the internal rules of operation, 2nd Edition of 27.6.2017.

2 the term certification authority < > should be replaced by a service provider < >.

Findings: Policy documents arranged in AC internal rules of operation, public part of NLB, 2nd Edition of 27.6.2017, AC Confidential part of the internal rules of operation of NLB, 2nd Edition of 27.6.2017.

3 the procedure for the management of complaints and resolution of disputes should be included in the public policy AC NLB.

Conclusion: arranged in document Policy AC public internal rules of operation of NLB, 2nd Edition of 27.6.2017.

4 Instructions for dealing with customer complaints, a guide to the process of managing customer complaints in February 2017 – should be defined, in order to appeal may be forwarded to the contact information.

Conclusion: arranged in document Policy AC public internal rules of operation of NLB, 2nd Edition of 27.6.2017.

5 identify the necessary safety tests-tests and penetracijskih tests in literature, CA.

Conclusion: Taken Care Of.

6 Penetracijski_testi_ACNLB 14.6.2017 Document must contain a period of implementation.

Conclusion: Taken Care Of.

2.3 findings and minor non-conformities

The above conclusions and/or minor non-conformities, bring no major discrepancies. However, their neglect can lead to inefficiencies in the management of services, which can lead to a rise in non-compliance with EIDAS or the relevant ETSI standards. These findings and/or minor non-conformities are organizational opportunities to improve the management of the service of the faith.

The organisation must analyse the findings and/or minor non-compliances that are listed below and provide answers as to how they will be eliminated. The Organization must draw up a plan for the realization of the adopted findings and/or minor non-compliance and to provide a proper answer taking into account the findings and/or minor inconsistencies.

1 the process of switching to TLS 1.2 should be done on the basis of the test.

Conclusion: the implementation of the Plan will be prepared after the completion of the test the vulnerabilities in 2017.

3 CONCLUSION

The auditor confirms that MTS carries out, maintain and develop good security CA practices that are consistent with the eIDAS-electronic identification and services trust, and ETSI standards.

The effectiveness of the implemented measures shall be verified at the next audit review, not later than the date of **28 June 2019**.

Annex:

- Checklist
- Open the assessment

Copies of:

- 1 x sponsor
- 1 x SIQ archive