Ernst & Young spółka z ograniczoną odpowiedzialnością
Business Advisory spółka komandytowa
Rondo ONZ 1
00-124 Warszawa

+48 22 557 70 00
+48 22 557 70 01
warszawa@pl.ey.com
www.ey.com/pl

Building a better working world

INDEPENDENT ASSURANCE REPORT

To the Management of Krajowa Izba Rozliczeniowa S.A.:

Scope

We have been engaged, in a reasonable assurance engagement, to report on Krajowa Izba Rozliczeniowa S.A (“KIR”) management’s assertion that for its Certification Authority (CA) services in Warsaw, Poland known as Centrum Obsługi Podpisu Elektroniczego SZAFIR (SZAFIR CA) for the ROOT CA: SZAFIR ROOT CA, SZAFIR ROOT CA2, throughout the period December 19, 2017 to December 18, 2018 for its CAs as enumerated in Appendix A, KIR has:

- disclosed its SSL certificate lifecycle management business practices in its:
  - Certification Practice Statement; and
  - Certificate Policy

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Krajowa Izba Rozliczeniowa S.A. website, and provided such services in accordance with its disclosed practices

- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and
  - SSL subscriber information is properly authenticated (for the registration activities performed by Krajowa Izba Rozliczeniowa S.A.)

- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

And, for its CAs as enumerated in Appendix A:

- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

in accordance with the *WebTrust$^{SM/TM}$ Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.3*.

Certification authority's responsibilities

Krajowa Izba Rozliczeniowa S.A.'s management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the *WebTrust$^{SM/TM}$ Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.3*.

Our independence and quality control

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior.

The firm applies International Standard on Quality Control 1, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Auditor's responsibilities

Our responsibility is to express an opinion on management's assertion based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, Assurance Engagements Other than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion is fairly stated, and, accordingly, included:

(1) obtaining an understanding of Krajowa Izba Rozliczeniowa S.A.'s SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL certificates, and obtaining an understanding of Krajowa Izba Rozliczeniowa S.A.'s network and certificate system security to meet the requirements set forth by the CA/Browser Forum;
(2) selectively testing transactions executed in accordance with disclosed SSL certificate lifecycle management practices;
(3) testing and evaluating the operating effectiveness of the controls; and
(4) performing such other procedures as we considered necessary in the circumstances.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Relative effectiveness of controls

The relative effectiveness and significance of specific controls at Krajowa Izba Rozliczeniowa S.A. and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Inherent limitations

Because of the nature and inherent limitations of controls, Krajowa Izba Rozliczeniowa S.A.'s ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

Opinion

In our opinion, throughout the period December 19, 2017 to December 18, 2018, Krajowa Izba Rozliczeniowa S.A. management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with the *WebTrust$^{SM/TM}$ Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.3*.

This report does not include any representation as to the quality of Krajowa Izba Rozliczeniowa S.A.'s services beyond those covered by the *WebTrust$^{SM/TM}$ Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.3*, nor the suitability of any of Krajowa Izba Rozliczeniowa S.A.'s services for any customer's intended purpose.

Use of the WebTrust seal

Krajowa Izba Rozliczeniowa S.A.'s use of the WebTrust for Certification Authorities – SSL Baseline with Network Security Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

EY, Warsaw, Poland

March 4, 2019

Management's Assertion Regarding the Effectiveness of Its Controls Over the SSL Certification Authority (CA) Based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3

March 4, 2019

We, as the management of Krajowa Izba Rozliczeniowa S.A. (KIR), are responsible for operating the SSL Certification Authority (CA) services in Warsaw, Poland for the SZAFIR ROOT CA and SZAFIR ROOT CA2 in scope for SSL Baseline Requirements and Network Security Requirements listed at Appendix A.

Controls have inherent limitations, including the possibility of human error and the circumvention or overriding of controls. Accordingly, even effective controls can provide only reasonable assurance with respect to Krajowa Izba Rozliczeniowa S.A.'s CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

The management of Krajowa Izba Rozliczeniowa S.A. has assessed the disclosure of its certificate practices and its controls over its SSL Certificate Authority (CA) services. Based on that assessment, in providing its SSL Certification Authority (CA) services in Warsaw, Poland throughout the period from December 19, 2017 through December 18, 2018, Krajowa Izba Rozliczeniowa S.A. has:

- Disclosed its SSL certificate lifecycle management business practices in its;
  - Certification Practice Statement; and
  - Certificate Policy

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Krajowa Izba Rozliczeniowa S.A. website, and provided such services in accordance with its disclosed practices

- Maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and SSL certificates it manages was established and protected throughout their lifecycles; and
  - SSL subscriber information was properly authenticated (for the registration activities performed by Krajowa Izba Rozliczeniowa S.A.)

- Maintained effective controls to provide reasonable assurance that:
  - Logical and physical access to CA systems and data was restricted to authorized individuals;
  - The continuity of key and certificate management operations was maintained; and

- Maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

for the Root CA(s) in scope for SSL Baseline Requirements and Network Security Requirements at Appendix A, based on the WebTrust[SM/TM] Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.3.

Management of Krajowa Izba Rozliczeniowa S.A.

Appendix A

CA	CERT	SUBJECT	ISSUER	SERIAL NUMBER	KEY ALGORITHM	KEY SIZE	SIGNATURE ALGORITHM	NOT BEFORE	NOT AFTER	SUBJECT KEY IDENTIFIER	SHA-256 FINGERPRINT
1	1	CN = SZAFIR ROOT CA O = Krajowa Izba Rozliczeniowa S.A. C = PL	CN = SZAFIR ROOT CA O = Krajowa Izba Rozliczeniowa S.A. C = PL	00 e6 09 fe 7a ea 00 68 8c e0 24 b4 ed 20 1b 1f ef 52 b4 44 d1	rsaEncryption	(2048 bits)	sha1RSA	Dec 6 12:10:57 2011	Dec 6 12:10:57 2031	53 92 a3 7d ff 82 76 f0 33 d4 eb 92 67 47 61 33 1b 68 3b 2a	fa bc f5 19 7c dd 7f 45 8a c3 38 32 d3 28 40 21 db 24 25 fd 6b ea 7a 2e 69 b7 48 6e 8f 51 f9 cc
1	2	CN = SZAFIR ROOT CA2 O = Krajowa Izba Rozliczeniowa S.A. C = PL	CN = SZAFIR ROOT CA2 O = Krajowa Izba Rozliczeniowa S.A. C = PL	3e 8a 5d 07 ec 55 d2 32 d5 b7 e3 b6 5f 01 eb 2d dc e4 d6 e4	rsaEncryption	(2048 bits)	sha256RSA	Oct 19 08:43:30 2015	Oct 19 08:43:30 2035	2e 16 a9 4a 18 b5 cb cc f5 6f 50 f3 23 5f f8 5d e7 ac f0 c8	a1 33 9d 33 28 1a 0b 56 e5 57 d3 d3 2b 1c e7 f9 36 7e b0 94 bd 5f a7 2a 7e 50 04 c8 de d7 ca fe