Shape the future with confidence

Ernst & Young
Audyt Polska sp. z o.o. sp.k.

Rondo ONZ 1
00-124 Warszawa

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

INDEPENDENT ASSURANCE REPORT

To the Management of Krajowa Izba Rozliczeniowa S.A. (KIR):

Scope

We have been engaged, in a reasonable assurance engagement, to report on KIR Management's Assertion that for its Certification Authority (CA) operations in Warsaw, Poland, and supporting facilities in Warsaw District, Poland, throughout the period April 9, 2025 to April 8, 2026, for its CAs as enumerated in Attachment A, KIR has:

- disclosed its TLS certificate lifecycle management business practices in its:
  - Certification Practice Statement version 1.23 valid until November 30, 2025;
  - Certification Practice Statement version 1.24 valid until January 11, 2026;
  - Certification Practice Statement version 1.25 valid until March 13, 2026;
  - Certification Practice Statement version 1.26; and
  - Certificate Policy version 1.14 valid until January 11, 2025;
  - Certificate Policy version 1.15;
  - Certification Practice Statement and Certification Policy of KIR for Trusted Non-Qualified TLS Certificates version 1.0;

  including its commitment to provide TLS certificates in conformity with the CA/Browser Forum Requirements on the KIR website, and provided such services in accordance with its disclosed practices

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

- 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

in accordance with the WebTrust Principles and Criteria for Certification Authorities – TLS Baseline v2.10.

The CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates require the CA to operate controls to adhere to the Network and Certificate System Security Requirements. The WebTrust Principles and Criteria for Certification Authorities – Network Security address this requirement and are reported on in a separate report.

Certification Authority's responsibilities

KIR'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 Principles and Criteria for Certification Authorities – TLS Baseline v2.10.

Shape the future
with confidence

Our independence and quality management

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 behaviour.

The firm applies International Standard on *Quality Management (ISQM) 1, Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* which require the firm to design, implement and operate a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Practitioner'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 (Revised), *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 KIR's TLS certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of TLS certificates;
2) selectively testing transactions executed in accordance with disclosed TLS 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.

As part of our engagement, we assessed the attached matters (Attachment B) that have been publicly posted by KIR management in the online forums of the Bugzilla site, as well as the online forums of individual internet browsers that comprise the CA/Browser Forum. We have considered the nature of these issues, their root causes, and CA's remediation plans in determining the nature, timing, and extent of our procedures.

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

The relative effectiveness and significance of specific controls at KIR 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

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. For example, because of their nature, controls may not prevent, or detect unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection to the future of any conclusions based on our findings is subject to the risk that controls may become ineffective.

Shape the future
with confidence

Opinion

In our opinion, throughout the period April 9, 2025 to April 8, 2026, KIR Management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – TLS Baseline v2.10.

This report does not include any representation as to the quality of KIR's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – TLS Baseline v2.10, nor the suitability of any of KIR's services for any customer's intended purpose.

Use of the WebTrust seal

KIR's use of the WebTrust for Certification Authorities – TLS Baseline 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.

Anna Wolak
EY, Warsaw, Poland

Podpisane elektronicznie przez Anna Magdalena Wolak

(Certyfikat kwalifikowany) w dniu 2026-05-29.

May 29, 2026

KRAJOWA IZBA ROZLICZENIOWA S.A.'S MANAGEMENT ASSERTION

Krajowa Izba Rozliczeniowa S.A. (KIR) operates the Certification Authority (CA) services as enumerated in **Attachment A**, and provides TLS CA services.

The management of KIR is responsible for establishing and maintaining effective controls over its TLS CA operations, including its TLS CA business practices disclosure on its website https://www.elektronicznypodpis.pl/, TLS key lifecycle management controls, and TLS certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to KIR's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

KIR management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in providing its TLS Certification Authority (CA) services in Warsaw, Poland, and supporting facilities in Warsaw District, Poland, throughout the period April 9, 2025 to April 8, 2026, KIR has:

- disclosed its TLS certificate lifecycle management business practices in its:
  - Certification Practice Statement version 1.23 valid until November 30, 2025;
  - Certification Practice Statement version 1.24 valid until January 11, 2026;
  - Certification Practice Statement version 1.25 valid until March 13, 2026;
  - Certification Practice Statement version 1.26; and
  - Certificate Policy version 1.14 valid until January 11, 2025;
  - Certificate Policy version 1.15;
  - Certification Practice Statement and Certification Policy of KIR for Trusted Non-Qualified TLS Certificates version 1.0;

  including its commitment to provide TLS certificates in conformity with the CA/Browser Forum Requirements on KIR website, and provided such services in accordance with its disclosed practices

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

- 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

in accordance with the WebTrust Principles and Criteria for Certification Authorities – TLS Baseline v2.10

Management of Krajowa Izba Rozliczeniowa S.A.

Wojciech Pantkowski - Vice President

Signed by /
Podpisano przez:

Wojciech Janusz
Pantkowski

Date / Data: 2026-
05-29 14:46

Sylwia Gajderowicz - Commercial Proxy

Podpisano przez/ Signed by:
SYLWIA
GAJDEROWICZ
Data/ Date: 29.05.2026 14:40
mSzafir

.....
May 29, 2026

Ernst & Young
Audyt Polska sp. z o.o. sp.k.
Rondo ONZ 1
00-124 Warszawa

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

Shape the future with confidence

KIR CERTIFICATION AUTHORITY

Attachment A: List of CAs in Scope

Subject	Issuer	SERIAL NUMBER	KEY ALGORITHM	KEY SIZE	SIGNATURE ALGORITHM	NOT BEFORE	NOT AFTER	SUBJECT KEY IDENTIFIER	SHA-256 Hash (Certificate)	Revoked status
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	6.12.2011	6.12.2031	53 92 A3 7D FF 82 76 F0 33 D4 EB 92 67 47 61 33 1B 68 3B 2A	FABCF5197CDD7F458AC33832D3284021DB2425FD6BEA7A2E69B7486E8F51F9CC	revoked
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	19.10.2015	19.10.2035	2E 16 A9 4A 18 B5 CB CC F5 6F 50 F3 23 5F F8 5D E7 AC F0 C8	A1339D33281A0B56E557D3D32B1CE7F9367EB094BD5FA72A7E5004C8DED7CAFE	
CN = SZAFIR Trusted CA2 O = Krajowa Izba Rozliczeniowa S.A. C = PL	CN = SZAFIR ROOT CA2 O = Krajowa Izba Rozliczeniowa S.A. C = PL	77 59 4f bb 22 70 38 fb 52 09 7e 61 a2 b7 f8 85 05 4c 4f 7b	rsaEncryption	2048 bits	sha256RSA	26.10.2015	26.10.2025	1E 75 BC 33 A3 1F 6A CC 7E CF DD 05 3E DB BB DA 7C BC E9 44	E22E6B25908E1107A607AF060E0B24E50C6D9562FF04F455BE0F8DF41A5032C0	
CN = SZAFIR Trusted CA6 O = Krajowa Izba Rozliczeniowa S.A. C = PL	CN = SZAFIR ROOT CA2 O = Krajowa Izba Rozliczeniowa S.A. C = PL	16 86 d6 6e 49 97 41 c3 58 f3 61 fe 25 33 16 09 10 f1 b5 74	rsaEncryption	4096 bits	sha256RSA	21.10.2024	21.10.2034	04 02 E4 05 49 01 F7 DE 77 BF EB FB 85 BF 1F 44 CC 3E F1 B4	8DBCEFD897D49653085E8914E71664943C2BC674405193B3AFAB3F66E92AD961	
CN = SZAFIR ROOT CA3 TLS O = Krajowa Izba Rozliczeniowa S.A. C = PL	CN = SZAFIR ROOT CA3 TLS O = Krajowa Izba Rozliczeniowa S.A. C = PL	30 1F 10 47 FD 02 19 2C C8 66 29 D2 D3 88 9B CF A9 B7 06 3A	rsaEncryption	4096 bits	SHA512WithRSA	18.03.2026	18.03.2041	F6 9E 0F 92 BC E2 D6 94 BE AE 5E BB 25 76 BE 9D 6B 45 67 7A	3032055A2617521DCBDED330A5161BF067611CFD2A6A01932705BA9B0C30ABC8	

EY in Poland is A Member Practice of EY Global
District Court for the City of Warsaw, Economic Dept., XII of the National Court Register,
KRS: 0000481039, NIP: 526-020-79-76
Registered Office: Rondo ONZ 1, 00-124 Warszawa

CN = SZAFIR Trusted CA7 TLS OV O = Krajowa Izba Rozliczeniowa S.A. C = PL	CN = SZAFIR ROOT CA3 TLS O = Krajowa Izba Rozliczeniowa S.A. C = PL	12 3D F0 78 41 39 E9 D6 11 BD 5E 4B 2D 38 08 1B CD 2B 99 13	rsaEncryption	4096 bits	SHA512WithRSA	27.03.2026	27.03.2031	5C 7A E0 64 45 21 11 3C 95 B2 0A F7 C2 FD 0C C5 1C 00 F2 4B	8FCCF1B288E18CE663C8E24485E2F2513A63C4582E5ADB1965598462466C4809	

Shape the future with confidence

Ernst & Young
Audyt Polska sp. z o.o. sp.k.
Rondo ONZ 1
00-124 Warszawa

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

Attachment B: List of Bugzilla issues noted during the period under review.

Mozilla Bug # Link	Description	Date Reported	Date Resolved	Criteria
1967929	Two CPRs were sent to by the Chrome Root Program Team on May 2, 2025 (~14:09 UTC) using the KIR problem reporting address disclosed to the CCADB. Further, on May 5, 2025 (~13:07 UTC) to the CA Email Alias address disclosed to the CCADB, but KIR failed to respond within the time requirement of Section 4.9.5 of the TLS BRs. Remediation Description: KIR CA Email Alias address disclosed to the CCADB was updated on 28.05.2025 to contain all and only persons from WebPKI team. Later, on 01.06.2025 KIR problem reporting address disclosed to the CCADB was updated to be dedicated email address for certificate problem reporting for fast processing within 24 hours. On 05.06.2025 an internal procedure was introduced for quarterly check of correctness and completeness of email group addresses.	22.05.2025	17.07.2025	TLS 2.5.2
1966006	The revocation of subordinate CA certificate Szafir Trusted CA3 was not disclosed to the CCADB within timeline required by Section 6 of the Chrome Root Program Policy and CCADB Policy (section 4. Subordinate CA Certificates). The issue was first noticed and reported by The Chrome Root Program (CRP) Team. Remediation Description: Operational procedure for disclosure/updating statuses to CCADB was updated on 13.05.2025. Training for WebPKI team was done and a monthly review of entries in the CCADB database (and after any major change in the PKI system) was introduced on 21.05.2025.	13.05.2025	01.07.2025	N/A

EY in Poland is A Member Practice of EY Global
District Court for the City of Warsaw, Economic Dept., XII of the National Court Register,
KRS: 0000481039, NIP: 526-020-79-76
Registered Office: Rondo ONZ 1, 00-124 Warszawa