

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 of time from April 9, 2024 to April 8, 2025, for its CAs as enumerated in **Appendix A**, KIR has:

- ▶ disclosed its SSL certificate lifecycle management business practices in its:
 - [Certification Practice Statement version 1.23](#), and
 - [Certificate Policy version 1.14](#);including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the KIR's 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 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
- ▶ 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 Principles and Criteria for Certification Authorities - SSL Baseline v2.8](#).

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 - SSL Baseline v2.8.

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 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 SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL certificates, and obtaining an understanding of KIR'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.

KIR management has disclosed to us the attached matters (Attachment B) that have been posted publicly 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 comments 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.

Opinion

In our opinion, throughout the period of time from April 9, 2024 to April 8, 2025, 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 - SSL Baseline v2.8.

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 - SSL Baseline v2.8, 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 - SSL 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 2025-06-13.

June 13th, 2025

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 SSL CA services.

The management of KIR is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its website <https://www.elektronicznypodpis.pl/>, CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls and certificate lifecycle management controls and subordinate CA 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 SSL CA services. Based on that assessment, in providing its SSL Certification Authority (CA) services in Warsaw, Poland, and supporting facilities in Warsaw District, Poland, throughout the period April 9, 2024 to April 8, 2025, KIR has:

- disclosed its SSL certificate lifecycle management business practices in its:
 - [Certification Practice Statement version 1.23](#), and
 - [Certificate Policy version 1.14](#);including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements, 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 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
- 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 the [WebTrust Principles and Criteria for Certification Authorities – SSL Baseline v2.8](#).

Management of Krajowa Izba Rozliczeniowa S.A.

.....
June 13th, 2025

Podpisano przez/ Signed by:
SYLWIA
GAJDEROWICZ
Data/ Date: 13.06.2025 11:24




Signed by /
Podpisano przez:
Wojciech Janusz
Pantkowski
Date / Data: 2025-
06-13 11:58

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	2011-12-06	2031-12-06	53 92 A3 7D FF 82 76 F0 33 D4 EB 92 67 47 61 33 1B 68 3B 2A	FABCF5197CDD7F458AC33 832D3284021DB2425FD6B EA7A2E69B7486E8F51F9C C	
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	2015-10-19	2035-10-19	2E 16 A9 4A 18 B5 CB CC F5 6F 50 F3 23 5F F8 5D E7 AC F0 C8	A1339D33281A0B56E557D 3D32B1CE7F9367EB094BD 5FA72A7E5004C8DED7CAF E	
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	2015-10-26	2025-10-26	1E 75 BC 33 A3 1F 6A CC 7E CF DD 05 3E DB BB DA 7C BC E9 44	E22E6B25908E1107A607A F060E0B24E50C6D9562FF 04F455BE0F8DF41A5032C 0	
CN = SZAFIR Trusted CA3 O = Krajowa Izba Rozliczeniowa S.A. C = PL	CN = SZAFIR ROOT CA2 O = Krajowa Izba Rozliczeniowa S.A. C = PL	7e 4e e2 f8 6d 2a 11 80 e9 c9 1e a2 0f d9 11 2f 63 dc 54 52	rsaEncryption	4096 bits	sha256RSA	2023-11-10	2033-11-10	E5 64 25 EA 97 8E 21 A4 C1 B6 2F 28 C9 70 0A 92 44 5E 6C 64	EC036C294F512DD28C566 6C2D53EC0DC6F397FED6 F8703A7C7532DA3E02DE8 C	revoked

CN = SZAFIR Trusted CA4 O = Krajowa Izba Rozliczeniowa S.A. C = PL	CN = SZAFIR ROOT CA2 O = Krajowa Izba Rozliczeniowa S.A. C = PL	7b 4e 10 c4 23 7b 28 9c 82 fc fc fe 28 20 fa ef 15 18 8f b8	rsaEncryption	4096 bits	sha256RSA	2024-09-16	2034-09-16	69 8F 1B CD 8E 44 93 B8 48 49 0F 3D 42 3F 89 57 48 95 43 5A	1FDC53B2632136B0331F2 1E88BD922DF4F1A37E90D 1D7003E266BA51A22DD6 0A	revoked
CN = SZAFIR Trusted CA5 O = Krajowa Izba Rozliczeniowa S.A. C = PL	CN = SZAFIR ROOT CA2 O = Krajowa Izba Rozliczeniowa S.A. C = PL	6e 6c 60 b8 10 ff 51 3d b5 48 40 93 21 da 19 b1 b5 ab a2 6c	rsaEncryption	4096 bits	sha256RSA	2024-10-08	2034-10-08	7F FB E2 57 E2 02 60 3E D3 FF B8 51 4F 9E 7F AB 95 A3 16 F9	1EBFA14EBD05CB7CAA79F 84F4992379F1497AADD9E D0C7784B320411038292E E	
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	2024-10-21	2034-10-21	04 02 E4 05 49 01 F7 DE 77 BF EB FB 85 BF 1F 44 CC 3E F1 B4	8DBCEFD897D49653085E8 914E71664943C2BC67440 5193B3AFAB3F66E92AD96 1	

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

Mozilla Bug # Link	Description	Date Reported	Date Resolved	Criteria
1921598	"An incident occurred where 1 intermediate certificate was incorrectly issued. Certificate Policies extension in SZAFIR Trusted CA3 Intermediate CA were missing Reserved Certificate Policy Identifiers that indicate adherence and compliance with S/MIME BR . KIR was first notified by an email message from Rob Stradling posted to kontakt at kir.pl." "Incident Root Cause(s): The process for issuing intermediate CA certificates (unlike EE certificates) involved several manual steps and was based on dedicated procedure for CA generation. During the CA certificate generation on October 11, 2023 the updated procedure for CA generation contained an incorrect value in the Certiifcation Policy field. The operator during the generation ceremony performed actions according to the procedure and used the wrong value from the procedure. Remediation Description: Procedures for the generation of CA certificates to include all possible extensions and DN values were updated. KIR included an additional check by the dedicated person from compliance department to validate the procedure before the use to generate a certificate. All certificate profiles on KIR's CA system were reviewed and automatic linter for intermediate CA certificates checks was implemented. Migration plan and of impacted certificate has been executed Commitment Summary: All checks said above are in place. Migration plan of impacted certificate has been executed All Action Items disclosed in this Incident Report have been completed as described, and KIR requested its closure which was granted."	28-09-2024	19-02-2025	S/MIME
1921596	"An incident occurred where 2 issued intermediate certificates were incorrectly disclosed in ccadb via case instead of dedicated link in ccadb.	28-09-2024	19-02-2025	CPS/ CCADB

	KIR personnel were first notified by a email message from Rob Stradling posted to kontakt at kir.pl. At moment all affected certificates are correctly disclosed in ccadb" "Incident Root Cause(s): The operational procedure for disclosure to CCADB was too general and was not referencing the correct disclosure procedure directly https://www.ccadb.org/cas/intermediates#adding-intermediate-certificate-data that is why WebPKI team operator chose the wrong way to disclose the certificates in ccadb via case. Remediation Description: Oprational procedure for disclosure to CCADB was updated. Training for WebPKI team to use updated Oprational procedure for disclosure was performed. Commitment Summary: KIR personnel are going to keep their oprational procedure for disclosure certificates in CCADB up-to-date to prevent similar issue to occur. All Action Items disclosed in this Incident Report have been completed as described, and KIR requested its closure which was granted."			
1921597	"An incident occurred where 2 intermediate certificates were incorrectly issued. Certificate Policies extensions in SZAFIR Trusted CA4 Intermediate CA certificate were missing Reserved Certificate Policy Identifiers that indicate adherence and compliance with TLS BR. KIR was first notified by a email message from Rob Stradling posted to kontakt at kir.pl." "Incident Root Cause(s): The process for issuing intermediate CA certificates (unlike EE certificates) contained several manual steps and it was based on dedicated procedure for CA generation. During the CA certificate generation on Septepmber 16, 2024 the updated procedure for CA generation contained an incorrect value in the Certiifcation Policy field. The operator during the generation ceremony performed actions according to the procedure and used the wrong value from the procedure.	28-09-2024	19-02-2025	SSL

	Remediation Description: Procedures for the generation of CA certificates now include all possible extensions checks and DN values Additional check by the dedicated person from compliance department to validate the procedure before the use to generate a certificate Automatic linter for intermediate CA certificates was implemented Reviewed all certificate profiles on root CA system https://crt.sh/?caid=369967 has been revoked Commitment Summary: KIR's personnel are going to continue executing checks said above to prevent similar issue to occur All Action Items disclosed in this Incident Report have been completed as described, and KIR requested its closure which was granted."			
1950292	This bug is intended as a document repository for KIR S.A. Self-Assessments of compliance with various CA/B Forum Standards and Root Store Policies using CCADB templates listed in https://www.ccadb.org/cas/self-assessment. Not an actual bug, even though has been categorized as a bug.	25-02-2025	N/A	N/A
1922572	"KIR has issued SZAFIR Trusted CA3 Intermediate CA certificate with missing Reserved Certificate Policy Identifiers that indicate adherence and compliance with S/MIME BR as described in https://bugzilla.mozilla.org/show_bug.cgi?id=1921598 According to SBR [https://cabforum.org/uploads/CA-Browser-Forum-SMIMEBR-1.0.6.pdf] section 4.9.1.2 - The Issuing CA SHALL revoke a Subordinate CA Certificate within seven (7) days. This has not been completed. A full incident report was to be provided no later than Friday October 11th 2024." "Incident Root Cause(s): The main root cause for the delayed certificates revocation lies in the outages in critical infrastructure if given revocation would take place. The root casue can be dived into 2 issues: a) Issues with new chain in back-end systems b) Issues with subscribers' certificates Remediation Description: SZAFIR Trusted CA5 was put into operation. Remediation plan has been executed. Subscribers were educated, we enhanced	03-10-2024	08-05-2025	S/MIME

	their understanding of immediate revocation requirements, and facilitated them in preparing for a swift certificate replacement process, to ensure that the certificates can be replaced within the revocation deadline in case needed. They were also advised to get them off publicly trusted certificates or consider utilizing private PKI, and prepare other contingency plans for enforced certificate revocation to minimize disruptions to their systems. KIR has also planned to provide ARI extension to ACME. Commitment Summary: All checks said above are in place. All Action Items disclosed in this Incident Report have been completed as described, and KIR requested its closure which was granted. Additional comments: This case was specifically discussed during walkthroughs with the spotlight on additional comments in the Bugzilla report concerning this issue. KIR's personnel explained, that the root cause of the delay lies withing the client's systems and how the affected certificates were used, which caused delays in replacing them in a timely manner, which was beyond KIR's control."			
--	---	--	--	--