

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 statement 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, 2023 to April 8, 2024, for its CAs as enumerated in **Appendix A**, KIR has:

- ▶ disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
 - [Certification Practice Statement version 1.19](#) and
 - [Certificate Policy version 1.13](#)
- ▶ maintained effective controls to provide reasonable assurance that:
 - KIR's Certification Practice Statement is consistent with its Certificate Policy; and
 - KIR provides its services in accordance with its Certificate Policy and Certification Practice Statement
- ▶ maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
 - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
 - subscriber information is properly authenticated (for the registration activities performed by KIR); and
 - subordinate CA certificate requests are accurate, authenticated, and approved
- ▶ 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, v2.2.2](#)

KIR does not provide Subordinate CA [cross-]certification, Subscriber Key Management Services, CA Key Escrow, CA-Provided Subscriber Key Storage and Recovery Services. Accordingly, our report does not extend to controls that would address those criteria.

Certification Authority's responsibilities

KIR's Management is responsible for its statement, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities Version 2.2.2.

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, due care, confidentiality, and professional behavior.

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 statement 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 statement is fairly stated, and, accordingly, included:

- 1) obtaining an understanding of KIR's key and certificate lifecycle management business practices and its controls over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate lifecycle management operations and over development, maintenance and operation of systems integrity;
- 2) selectively testing transactions executed in accordance with disclosed key and certificate lifecycle management business 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 that there were no matters that have been posted publicly in the online forums of the Bugzilla site throughout the period of time from April 9, 2023 to April 8, 2024. We have considered the nature of this comment 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, 2023 to April 8, 2024, KIR management's statement, as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities Version 2.2.2.

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 Version 2.2.2, 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 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.

Jakub Walarus
EY, Warsaw, Poland

Natalia Dembek-Ślusarczyńska
EY, Warsaw, Poland

**Jakub Jerzy
Walarus**
Cyfrowo podpisane przez Jakub
Jerzy Walarus
DN: cn=Jakub Jerzy Walarus,
c=PL
Data: 2024.07.05 02:19:47
+02'00'

Podpisane elektronicznie przez
Natalia Dembek-Ślusarczyńska
(Certyfikat kwalifikowany) w dniu
2024-07-05.

July 5, 2024



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

Appendix A: List of CAs in Scope

CA	CERT	SUBJECT	ISSUER	SERIAL NUMBER	KEY ALGORITHM	KEY SIZE	SIGNATURE ALGORITHM	NOT BEFORE	NOT AFTER	SUBJECT KEY IDENTIFIER	SHA-256 FINGERPRINT	OTHER INFORMATION
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	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	FABCF5197CDD7F458AC33832D3284021DB2425FD6BEA7A2E69B7486E8F51F9CC	
2	1	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	A1339D33281A0B56E557D3D32B1CE7F9367EB094BD5FA72A7E5004C8DED7CAFE	
2	2	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	E22E6B25908E1107A607AF060E0B24E50C6D9562FF04F455BE0F8DF41A5032C0	
2	3	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	EC036C294F512DD28C5666C2D53EC0DCF6F397FED6F8703A7C7532DA3E02DE8C	

KRAJOWA IZBA ROZLICZENIOWA S.A.'S MANAGEMENT STATEMENT

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

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate suspension
- Certificate validation
- Certificate status information processing
- Subscriber key generation
- Integrated circuit card life cycle management

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 CA services. Based on that assessment, in KIR management's opinion, in providing its Certification Authority (CA) services in Warsaw, Poland, and supporting facilities in Warsaw District, Poland, throughout the period April 9, 2023 to April 8, 2024, KIR has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
 - [Certification Practice Statement version 1.19](#), and
 - [Certificate Policy version 1.13](#);
- maintained effective controls to provide reasonable assurance that:
 - KIR's Certification Practice Statement is consistent with its Certificate Policy;
 - KIR provides its services in accordance with its Certificate Policy and Certification Practice Statement;
- maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
 - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
 - subscriber information is properly authenticated (for the registration activities performed by KIR);
 - subordinate CA certificate requests are accurate, authenticated, and approved;

- 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 v2.2.2](#), including the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS)
- Certificate Policy (CP)

CA Business Practices Management

- Certificate Policy Management
- Certification Practice Statement Management
- CP and CPS Consistency

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical & Environmental Security
- Operations Management
- System Access Management
- System Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Key Lifecycle Management Controls

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival and Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management

Subscriber Key Lifecycle Management Controls

- CA-Provided Subscriber Key Generation Services
- Integrated Circuit Card (ICC) Lifecycle Management
- Requirements for Subscriber Key Management

Certificate Lifecycle Management Controls

- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Suspension
- Certificate Validation

KIR does not provide Subordinate CA [cross-]certification, Subscriber Key Management Services, CA Key Escrow, CA-Provided Subscriber Key Storage and Recovery Services. Accordingly, our statement does not extend to controls that would address those criteria.

Management of Krajowa Izba Rozliczeniowa S.A.



Signed by /
Podpisano przez:

Wojciech Janusz
Pantkowski

Date / Data:
2024-07-03 09:27



Signed by /
Podpisano przez:

Sylwia
Gajderowicz

Date / Data:
2024-07-03 09:39

July 3rd, 2024

KIR CERTIFICATION AUTHORITY

Attachment A: List of CAs in Scope

CA	CERT	SUBJECT	ISSUER	SERIAL NUMBER	KEY ALGORITHM	KEY SIZE	SIGNATURE ALGORITHM	NOT BEFORE	NOT AFTER	SUBJECT KEY IDENTIFIER	SHA-256 FINGERPRINT	OTHER INFORMATION
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	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	FABCF5197CDD7F458AC33832D3284021DB2425FD6BEA7A2E69B7486E8F51F9CC	
2	1	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	A1339D33281A0B56E557D3D32B1CE7F9367EB094BD5FA72A7E5004C8DED7CAFE	
2	2	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	E22E6B25908E1107A607AF060E0B24E50C6D9562FF04F455BE0F8DF41A5032C0	
2	3	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	EC036C294F512DD28C5666C2D53EC0DCF6F397FED6F8703A7C7532DA3E02DE8C	