Conformity Assessment Report:
Conformity Certificate and Summary

TelekomSecurity.031.0300.06.2023

Trust Service Provider:

Krajowa Izba Rozliczeniowa S.A.

Conformity Certificate

TelekomSecurity.031.0300.06.2023

pursuant to Article 20 par. 1 of REGULATION (EU) No. 910/2014[1]

valid from 01.07.2023 up to and including: 30.06.2025

Certification Body of Deutsche Telekom Security GmbH

Bonner Talweg 100, 53113 Bonn

This is to certify
– pursuant to Article 20 par. 1 of REGULATION (EU) No. 910/2014 –
that the

Trust Service Provider
„Krajowa Izba Rozliczeniowa S.A.“

provides the following trust services:

- **creating qualified certificates for electronic signatures**
- **creating qualified certificates for electronic seals**
- **creating qualified certificates for website authentication**
- **creating qualified electronic timestamps**
- **remote QSCD management for qualified el. signatures**

in accordance with the requirements of REGULATION (EU) No. 910/2014.

This certificate is filed and registered under: **TelekomSecurity.031.0300.06.2023**

Dokument unterschrieben
von: Dr. Furgel, Igor
am: 02.06.2023 11:32
Ort: Bonn

Bonn, 02.06.2023

i.V. Dr. Igor Furgel
Head of Certification Body

T CERTIFICATION BODY

Deutsche Telekom Security GmbH – Certification Body – is an accredited Conformity Assessment Body (CAB).
DAkkS Registration No.: D-ZE-21631-01 (former Certification Body of T-Systems International GmbH, former registration no.: D-ZE-12025-01).

DAkkS Deutsche Akkreditierungsstelle D-ZE-21631-01-00

[1] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

1. Object of the conformity assessment

1.1 Name of the trust service provider

Krajowa Izba Rozliczeniowa S.A.
Departament Kontaktów z Klientami i Operacji [Customer Service Point]

ul. rtm. W. Pileckiego 65
02 - 781 Warszawa
Poland

with the annotation reading “usługi zaufania” [trust services]

tel. 0-801 500 207
e-mail: kontakt@kir.pl

1.2 Current confirmation status

Krajowa Izba Rozliczeniowa S.A. (abbreviated as KIR) is a qualified trust service provider (qTSP) according to Art. 24 of eIDAS Regulation[2].

The last full conformity assessment according to Article 20(1) of eIDAS Regulation was accomplished with issuing the conformity certificate TelekomSecurity.031.0280.06.2021 as of 29.06.2021.

The current - 24 months periodic - conformity assessment of the TSP according to §20(1) eIDAS Regulation serves the continuation of its status as a ‘qualified trust service provider’ according to Article 24 eIDAS Regulation for all qualified trust services offered by the qTSP.

Current assessment is based on the TSP Certification Policy: “KIR CERTIFICATION POLICY FOR QUALIFIED TRUST SERVICES”, version 1.5 as of 21.12.2022. This document is publicly available under https://www.elektronicznypodpis.pl/en/ (“Information” -> “Legal basis”).

[2] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

2. TSP's trust services in scope of the conformity assessment

Krajowa Izba Rozliczeniowa S.A. operates and provides the following trust services in the qualified TSP operation as defined in eIDAS Regulation, Article 3

- creating qualified certificates for electronic signatures (qualified trust service – CA/QC),
- creating qualified certificates for electronic seals (qualified trust service - CA/QC),
- creating qualified certificates for website authentication (qualified trust service - CA/QC),
- creating qualified electronic timestamp (qualified trust service – TSA/QTST).

The TSP also provides qualified remote (server) signing service for TSP's subscribers for generation qualified electronic signatures, i.e.

- generating and managing signature creation data on behalf of the subscribes (qualified trust service – RemoteQSCDManagement/Q), and
- generating qualified electronic signatures based on signature creation data managed by TSP on behalf of subscribers (qualified trust service – RemoteQSCDManagement/Q).

The remote signing service for TSP's subscribers corresponds with the particular trust service type for remote signing
URI: http://uri.etsi.org/TrstSvc/Svctype/RemoteQSCDManagement/Q as defined by ETSI TS 119 612 v2.2.1, sec. 5.5.1.1.

TSP Certification Policy defines the policy identifiers for these qualified services as follows:

qualified service	policy identifiers
qualified certificates for electronic signature	iso(1) member-body(2) pl (616) organization(1) id-kir(113571) id-szafir(1) id-kw szafir-osoba fizyczna(1)
qualified certificates for electronic seal	iso(1) member-body(2) pl (616) organization(1) id-kir(113571) id-szafir(1) id-kw szafir-osoba prawna(3)

qualified service	policy identifiers
qualified certificates for websites authentication	iso(1) member-body(2) pl (616) organization(1) id-kir(113571) id-szafir(1) id-kw szafir-witryna(4)
qualified certificates for electronic signature where the signature creation data are managed by TSP (remote signing)	iso(1) member-body(2) pl (616) organization(1) id-kir(113571) id-szafir(1) id-kw mszafir-podpis(5)

Krajowa Izba Rozliczeniowa S.A. operates and provides the following relevant additional services:

- Registration (request submission, request verification, subscriber identification)

- Subscriber's key pair generation, if requested;
  the certificate may be issued with a pair of keys generated by TSP or to a public key from a pair generated by the subscriber

- Subscriber's public key certification (certificate production) for qualified electronic signatures, seals and website authentication

  The certificate extension qcStatement – qcSCD (information about storage of subscriber's keys in the qualified signature/seal creation device), is placed by the TSP in a qualified certificate, only under the conditions stated in chap. 4.2.3 "Certificate Generation" of the TSP Certification Policy "KIR CERTIFICATION POLICY FOR QUALIFIED TRUST SERVICES", version 1.5 as of 21.12.2022 (publicly available, see chap. 1.2 above).

  In any other cases (for example, if a key pair is generated by subscriber without the attendance of TSP Operator) the TSP does not check if the keys are stored in a qualified electronic signature creation device, and do not place qcStatement extension – qcSCD in the certificate.

- Personalization of the respective subscriber's qualified secure signature/seal creation devices (qSCD), i.e. linking the key pair for electronic signature/seal to subscriber (electronic personalisation), in case subscriber orders certificate with qualified secure signature creation device implemented as smartcard

- Certificate issuance / delivery of qSCD to subscriber

- Certificate suspension and revocation service

- Providing online certificate status information via OCSP (RFC 2560 on the request – response basis)

- Providing certificate status information by certificate revocation lists (CRLs)

- Operation of a web portal providing information about these services (www.elektronicznypodpis.pl/), including the TSP's Certification Policy , online forms for applications, subscriber information, legal basis, service certificates and CRLs and other related information

- Technical support hotline for customers/subscribers.

Following qualified trust services are covered by the current conformity assessment:

Description of the trust service	'qualified trust service type' according to ETSI TS 119 612 V2.1.1, sec. 5.5.1
creating qualified certificates for electronic signatures	URI: http://uri.etsi.org/TrstSvc/Svctype/CA/QC URI: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL/QC URI: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC
creating qualified certificates for electronic seals	URI: http://uri.etsi.org/TrstSvc/Svctype/CA/QC URI: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL/QC URI: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC
creating qualified certificates for website authentication	URI: http://uri.etsi.org/TrstSvc/Svctype/CA/QC URI: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL/QC URI: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC
creating qualified electronic timestamp	URI: http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Description of the trust service	‘qualified trust service type’ according to ETSI TS 119 612 V2.2.1, sec. 5.5.1 ETSI TS 119 612 V2.2.1 is NOT covered by the IMPLEMENTING DECISION (EU) 2015/1505 (Trusted Lists)
qualified remote qSCD management supports generation and management of signature creation data within qSCD(s) on behalf and under control of remote signers or seal creators	URI: http://uri.etsi.org/TrstSvc/Svctype/RemoteQSCDManagement/Q

Each qualified trust service covered by the current conformity assessment is identified by the service certificate information, which is unambiguously assignable to each single trust service.

This service certificate information is summarised below, whereby certificates tagged as ‘*for verification only*’ or ‘*expired*’, if any, shall be kept on trusted lists for enabling a long period verification[3].

The TSP operates the following PKIs:

A) PKI for CA “KIR_OZK62”

Service type identifier according to ETSI TS 119 612 V2.1.1, sec. 5.5.1:	URI: http://uri.etsi.org/TrstSvc/Svctype/CA/QC http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL/QC
Service name:	COPE SZAFIR Kwalifikowany
Root certificate (root CA)	

[3] It shall be noted that all service certificates for the 'qualified trust service type' http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST according to ETSI TS 119 612 V2.1.1 (sec. 5.5.1), which are marked as '*expired*', are no longer service indicating.

/C=PL /O= Narodowy Bank Polski	
certificate common name (CN)	**Serial number (SN)** **Fingerprint**
/CN= Narodowe Centrum Certyfikacji /organizationIdentifier = VATPL-5250008198	SN (hex): 40 f8 f7 8a b0 e3 64 10 56 91 c8 d9 e0 2c f8 c1 c6 40 0a 46 SN (dec): 370927558070677912140887258838452155756220254790 SHA1: 89 ce c4 84 2f af 40 1b 48 d0 f2 1d 80 43 e9 a6 3e 7c 02 d5
Trust service certificates /C = PL /O = Krajowa Izba Rozliczeniowa S.A.	
certificate common name (CN)	**Serial number (SN)** **Fingerprint**
/CN = COPE SZAFIR - Kwalifikowany /organizationIdentifier = VATPL-5260300517	*for verification only* *expiration date: 14.03.2028* *SN (hex): 60 f0 60 92 d2 30 9c 18 92 a9 c1 47 e1 86 ea f8 bc ad e3 02* *SN (dec): 553423705586801238687850233880118061903763071746* *SHA1: 54 9e af da 68 2c 26 52 da 28 e0 52 c5 71 43 c0 16 c4 b5 b3*
/CN = COPE SZAFIR - Kwalifikowany /organizationIdentifier = VATPL-5260300517	SN (hex): 06 2a ac 8d 84 b0 dd cc SN (dec): 444357237065965004 SHA1: 79 09 c7 b6 a7 c7 f9 95 f1 36 df 4b 96 c6 76 05 8f 90 7e 14 expiration date: 07.12.2032

Table 1: PKI certificates for the trust service /CA/QC and /Certstatus/CRL/QC (CA KIR_OZK62)

B) PKI for OCSP service (CA ’62’; CA ‘52’ was removed from the OCSP service, see below)

Service type identifier according to ETSI TS 119 612 V2.1.1, sec. 5.5.1:	URI: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC
Service name:	COPE SZAFIR Kwalifikowany
Root certificate (root CA) /C=PL /O=Narodowy Bank Polski	
certificate common name (CN)	**Serial number (SN)** **Fingerprint**
/CN= Narodowe Centrum Certyfikacji/organizationIdentifier = VATPL-5250008198	SN (hex): 40 f8 f7 8a b0 e3 64 10 56 91 c8 d9 e0 2c f8 c1 c6 40 0a 46 SN (dec): 370927558070677912140887258838452155756220254790 SHA1: 89 ce c4 84 2f af 40 1b 48 d0 f2 1d 80 43 e9 a6 3e 7c 02 d5
Trust service certificates /C = PL /O = Krajowa Izba Rozliczeniowa S.A.	
certificate common name (CN)	**Serial number (SN)** **Fingerprint**
/CN = COPE SZAFIR OCSP Responder OZK62	SN (hex): 52 45 1c 52 15 86 32 83 8c d8 86 75 8b db 44 4a d1 76 a6 46 SN (dec): 469678461702024211021229908508984033246797276742 SHA1: 2f b9 b1 0c be b4 38 6c 88 3c a8 2a af 6c 88 ff 72 29 b8 9b
/CN = COPE SZAFIR OCSP Responder OZK62	obsolete: *SN (hex):*

	76:b4:d2:a9:58:d9:85:f4:73:04:5e:e3:24:df :9e:d6:b5:c5:8e:72 *SHA1: ac c0 72 5d d1 34 73 c2 c1 8b a3 07 a2 23 24 db 8e c7 bf ba*
/CN = COPE SZAFIR OCSP Responder OZK62	obsolete: *SN (hex): 72 44 85 2b ab 41 81 48 2b 19 95 9e e6 01 34 6b a8 6d f5 ef* *SHA1: 97 bf 5f be c6 f2 01 8e 07 9f d5 42 ac 75 5c da 2c b1 95 96*

Table 2: PKI certificates for the trust service /Certstatus/OCSP/QC

C) PKI for CA "KIR_OZK52" (KIR_OZK52-1 and KIR_OZK52-2; this PKI instantiation is used exclusively for certificate revocation and for verification purposes; the last valid CRL is publicly available)

Service type identifier according to ETSI TS 119 612 V2.1.1, sec. 5.5.1:	URI: http://uri.etsi.org/TrstSvc/Svctype/CA/QC http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL/QC
Service name:	COPE SZAFIR Kwalifikowany
Root certificate (root CA) /C=PL /O=Minister wlasciwy do spraw gospodarki	
certificate common name (CN)	**Serial number (SN, hex)** **SHA1 Fingerprint**
/CN= Narodowe Centrum Certyfikacji (NCCert)/	62 a7 0d 04 c3 24 b8 d4 27 56 cc 3f 81 6b f2 eb 32 ef 07 19 a9 51 6f a8 11 53 5e 73 45 88 15 71 06 6c 77 0c f9 7f 66 95
Trust service certificates /SERIALNUMBER = Nr wpisu: 6 /C = PL /O = Krajowa Izba Rozliczeniowa S.A.	
certificate common name (CN)	**Serial number (SN, hex)** **SHA1 Fingerprint**
/CN = COPE SZAFIR - Kwalifikowany	50 af b7 64 da 75 ef ad eb 0f 08 d2 6a 6e 73 08 ea f2 c3 e2 3a 2b aa af aa cb 46 ee b8 67 6d d1 f2 a7

	4f e7 8a 92 83 8b

Table 3: PKI certificates for the trust service /CA/QC and /Certstatus/CRL/QC (CA KIR_OZK52-1) – for verification only

Service type identifier according to ETSI TS 119 612 V2.1.1, sec. 5.5.1:	URI: http://uri.etsi.org/TrstSvc/Svctype/CA/QC http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL/QC
Service name:	COPE SZAFIR Kwalifikowany
Root certificate (root CA) /C=PL/O=Minister wlasciwy do spraw gospodarki	
certificate common name (CN)	**Serial number (SN, hex)** **SHA1 Fingerprint**
/CN= Narodowe Centrum Certyfikacji (NCCert)	62 a7 0d 04 c3 24 b8 d4 27 56 cc 3f 81 6b f2 eb 32 ef 07 19 a9 51 6f a8 11 53 5e 73 45 88 15 71 06 6c 77 0c f9 7f 66 95
Trust service certificates SERIALNUMBER = Nr wpisu: 6 /C = PL /O = Krajowa Izba Rozliczeniowa S.A.	
certificate common name (CN)	**Serial number (SN, hex)** **SHA1 Fingerprint**
/CN = COPE SZAFIR - Kwalifikowany	63 b7 ce d1 91 6f fc a1 53 ca 84 7a 5f 57 a0 6d c6 a6 b2 ae 0a aa 6b 56 ef ca ac 69 41 fc 19 d0 bf e1 63 a1 7a 0d f2 83

Table 4: PKI certificates for the trust service /CA/QC and /Certstatus/CRL/QC (CA KIR_OZK52-2) – for verification only

D) PKI for “KIR TSA”

Service type identifier according to ETSI TS 119 612	URI: http://uri.etsi.org/TrstSvc/Svctype/TSA/Q

V2.1.1, sec. 5.5.1:	TST
Service name:	SZAFIR TSA
Root certificate (root CA) /C=PL /O=Narodowy Bank Polski	
certificate common name (CN)	**Serial number (SN)** **Fingerprint**
/CN= Narodowe Centrum Certyfikacji /organizationIdentifier = VATPL-5250008198	SN (hex): 40 f8 f7 8a b0 e3 64 10 56 91 c8 d9 e0 2c f8 c1 c6 40 0a 46 SN (dec): 370927558070677912140887258838452155756220254790 SHA1: 89 ce c4 84 2f af 40 1b 48 d0 f2 1d 80 43 e9 a6 3e 7c 02 d5
Trust service certificates /SERIALNUMBER = Nr wpisu: 11/ C=PL /O=Krajowa Izba Rozliczeniowa S.A.	
certificate common name (CN)	**Serial number (SN)** **Fingerprint**
/CN = SZAFIR TSA /organizationIdentifier (2.5.4.97) = VATPL-5260300517	*for verification only* *expiration date: 24.02.2029* *SN (hex): 15 58 41 6e 86 3a 56 eb b2 b4 77 2f 83 dc ad ae 4d 99 c0 2a* *SN (dec): 1218569716728367181787385292676059869118889820 58* *SHA1: 73 3c e9 ea c0 22 4a cf 0e fe b0 a6 7c f2 27 4f 37 5c 11 94*
/CN = SZAFIR TSA /organizationIdentifier (2.5.4.97) = VATPL-5260300517	SN (hex): 00 cb ec ec 5b 5c 61 42 SN (dec): 57399920161481026 SHA1: d2 ab 28 58 80 b6 f2 50 67 06 62 40

	65 f3 c0 f8 43 e0 d4 4d expiration date: 07.12.2032

Table 5: PKI certificates for the trust service /TSA/QTST (CA KIR_TSA)

In implementing the following services, Krajowa Izba Rozliczeniowa S.A. draws on the services of delegated third parties:

- Identification of subscribers and physical delivery of qSCDs to subscribers (by cooperating banks, only face-to-face physical presence identification procedure)
- Identification of subscribers using *mojeid.pl* service (by banks participating in the mojeid.pl service)
- Long-term records archiving.

A detailed information about the identification procedures and other customer related questions can be directly requested from the TSP.

3. Certification Programme

The current conformity assessment procedure has been performed in accordance with the Certification Program 031 ‘eIDAS TSP’ (accredited area) of the Certification Body of Deutsche Telekom Security GmbH (certification program 031)’.

The Certification Body of Telekom Security is a conformity assessment body as provided by Article 3 paragraph 18 of eIDAS. The Certification Body of T-Systems is accredited by the German Accreditation Authority (DAkkS; http://www.dakks.de/en, member of EA) for performing conformity assessment (audit) according to eIDAS requirements and according to ETSI EN 319 4xx / 5xx; accreditation ID: D-ZE-21631-01-00 (former D-ZE-12025-01-00).

4. Assessment of the TSP’s qualified operation

The current Certification Policy (version 1.5 as of 21.12.2022) of the trust service provider “Krajowa Izba Rozliczeniowa S.A.” is suitable for the operations of a qualified trust service provider as defined by eIDAS Regulation.

This Certification Policy of the trust service provider „Krajowa Izba Rozliczeniowa S.A.“ is implemented accordingly in practice.

The trust service provider „Krajowa Izba Rozliczeniowa S.A.“ operates the following trust services in compliance with the relevant requirements of the current version of eIDAS Regulation:

Description of the trust service	‘qualified trust service type’ according to ETSI TS 119 612 V2.1.1, sec. 5.5.1
creating qualified certificates for electronic signatures	URI: http://uri.etsi.org/TrstSvc/Svctype/CA/QC URI: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL/QC URI: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC
creating qualified certificates for electronic seals	URI: http://uri.etsi.org/TrstSvc/Svctype/CA/QC URI: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL/QC URI: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC
creating qualified certificates for website authentication	URI: http://uri.etsi.org/TrstSvc/Svctype/CA/QC URI: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL/QC URI: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC
creating qualified electronic timestamp	URI: http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Description of the trust service	‘qualified trust service type’ according to ETSI TS 119 612 V2.2.1, sec. 5.5.1 ETSI TS 119 612 V2.2.1 is NOT covered by the IMPLEMENTING DECISION (EU) 2015/1505 (Trusted Lists)
qualified remote qSCD management supports generation and management	URI: http://uri.etsi.org/TrstSvc/Svctype/RemoteQSCDManagement/Q

Description of the trust service	‘qualified trust service type’ according to ETSI TS 119 612 V2.2.1, sec. 5.5.1 ETSI TS 119 612 V2.2.1 is NOT covered by the IMPLEMENTING DECISION (EU) 2015/1505 (Trusted Lists)
of signature creation data within qSCD(s) on behalf and under control of remote signers or seal creators	

Table 6: Trust services provided in compliance with eIDAS Regulation

The qualified certificates profiles for electronic seals and website authentication comply with the relevant requirements of Article 34 of DELEGATED REGULATION (EU) 2018-389 in the context of Payment Services DIRECTIVE (EU) 2015-2366 (PSD2).

5. Integrated Modules

For implementing the trust services in scope, the TSP uses the following already eIDAS-confirmed qualified services provided by module operators as delegated third parties, whereby single certified and not certified operational options of the modules are exactly stated in each related Conformity Certificates for the modules.

A single module can be used by the TSP as *exclusive* or *non-exclusive* service provided by the respective delegated third party (called ‘module provider’).

In case of the *exclusive* service by a module, the TSP shall use the module for the provision of the qualified trust services listed in chap. 4, Table 6 above. Therefore, the present Conformity Certificate covers the operation of the qualified trust services listed in chap. 4, Table 6 above solely using the respective modules.

In case of the *non-exclusive* service by a module, the TSP may operatively decide on the usage or non-usage of the module in the qualified TSP operation. Hence, the present Conformity Certificate for the TSP covers the TSP operation with this service as well as without it.

The table below represents a snapshot at the time of issuance of the present Conformity Certificate. Precise information on the modules of the *non-exclusive*

services that are integrated by the VDA at a given time can be obtained from the TSP.

modul name	modul service	modul provider	address	Conformity Certificate acc. to eIDAS		exclusive or non-exclusive service by the module
				ID	valid until	
'EIM service – natural by PKO BP'	identification of *natural* persons i) in compliance with eIDAS Art. 24.1 (b) ii) confirmed assurance level: '*substantial*' acc. to Commission Implementing Regulation (EU) 2015/1502	PKO Bank Polski S.A.	ul. Puławska 15, 02-515 Warszawa, Poland	TelekomSecurity.031.0290.11.2021	13.11.2023	non-exclusive
'one-time EIM service – natural by ING Bank Śląski'	identification of *natural* persons i) in compliance with eIDAS Art. 24.1 (b) ii) confirmed assurance level: '*substantial*' acc. to Commission Implementing Regulation (EU) 2015/1502	ING Bank Śląski S.A.	ul. Sokolska 34, 40-086 Katowice, Poland	Telekom Security.031.0296.01.2023	31.08.2023	non-exclusive

modul name	modul service	modul provider	address	Conformity Certificate acc. to eIDAS		exclusive or non-exclusive service by the module
				ID	valid until	
'EIM service – natural by Pekao Bank S.A.'	identification of *natural* persons i) in compliance with eIDAS Art. 24.1 (b) ii) confirmed assurance level: '*substantial*' acc. to Commission Implementing Regulation (EU) 2015/1502	BANK POLSKA KASA OPIEKI S.A.	ul. Grzybowska 53/57, 00-844 Warszawa, Poland	Telekom Security.031.0298.01.2023	31.08.2023	non-exclusive
'EIM service – natural by mBank'	identification of *natural* persons i) in compliance with eIDAS Art. 24.1 (b) ii) confirmed assurance level: '*substantial*' acc. to Commission Implementing Regulation (EU) 2015/1502	mBank S.A.	ul. Prosta 18, 00-850 Warszawa, Poland	Telekom Security.031.0297.01.2023	01.02.2025	non-exclusive

6. Summary and Notes

1. The current Certification Policy of the trust service provider “Krajowa Izba Rozliczeniowa S.A.” – “KIR CERTIFICATION POLICY FOR QUALIFIED TRUST SERVICES”, version 1.5 as of 21.12.2022 – is suitable for the operation of a qualified trust service provider as defined by eIDAS Regulation and is implemented accordingly in practice.

2. The trust service provider „Krajowa Izba Rozliczeniowa S.A.“ operates the trust services listed in chap. 4, Table 6 above in compliance with the relevant requirements of the current version of eIDAS Regulation.

3. The qualified certificates profiles for electronic seals and website authentication comply with the relevant requirements of Article 34 of DELEGATED REGULATION (EU) 2018-389 in the context of Payment Services DIRECTIVE (EU) 2015-2366 (PSD2).

4. The present Conformity Certificate TelekomSecurity.031.0300.06.2023 is valid for the current Certification Policy up to and including 30.06.2025.
   This validity period (that is, the maximum possible duration of TSP operation in compliance with eIDAS Regulation) results from the specification of eIDAS Regulation, Article 20 (1).
   As the modules integrated into the qualified TSP operation do not provide any exclusive services and the TSP can therefore remove them from its operation (see Section 5), the validity period of the present Conformity Certificate is not affected by the validity period of the confirmations for these modules.
   The validity of the present Conformity Certificate can be extended or reduced if the basics upon which it was issued allow an extension or make a reduction necessary.

End of the Conformity Certificate

Conformity Certificate:
TelekomSecurity.031.0300.06.2023

Issuer:	Deutsche Telekom Security GmbH
Address:	Bonner Talweg 100, 53113 Bonn
Phone:	+49-(0)228-181-0
Fax:	+49-(0)228-181-49990
Web:	www.telekom-zert.com
	https://www.telekom.de/security