

General information about the CA's associated organization

CA Company Name	Krajowa Izba Rozliczeniowa S.A.
Website URL	www.kir.com.pl ; www.elektronicznypodpis.pl
Organizational type	Private corporation.
Primark Market / Customer Base	KIR S.A. is the one of the biggest Polish CAs which currently mainly issues qualified certificates for general public. Our certification is for non-qualified certificates only but our clients of qualified certificates are very interested in trusted non-qualified certificates. Since KIR S.A.'s is automated clearing house in Poland and its core business is clearings, KIR S.A. has built numerous contacts /business relationships within banking sector. Due to that fact, KIR S.A is aiming to expand its sales in services like: SSL or VPN certificates. KIR S.A's another line of products called PayByNet, has created a vast network of relationships within online stores and KIR S.A can leverage them to create customer base for trusted non-qualified certificates.
Impact to Mozilla Users	Types of Mozilla users who are likely to encounter our root certificate as relying parties: users of internet banking, online shops, clients of financial institutions e.g. insurance companies.
CA Contact Information CA Email Alias	CA Email Alias: przemyslaw.rawa@kir.com.pl CA Phone Number: +48 22 546 02 11 Title / Department: Deputy Director / Digital Signature Business Line

Technical information about each root certificate

Certificate Name	for root CA the name is: SZAFIR ROOT CA for sub CA the name is: SZAFIR Trusted CA
Certificate Issuer Field	for root CA: CN = SZAFIR ROOT CA, O = Krajowa Izba Rozliczeniowa S.A. for sub CA: CN = SZAFIR Trusted CA, O = Krajowa Izba Rozliczeniowa S.A.
Certificate Summary	SZAFIR ROOT CA is on the top of hierarchy, issues only certificates for sub CAs. SZAFIR Trusted CA is SZAFIR ROOT CA's subordinate CA, issues end-user certificates. SZAFIR Trusted CA issues 6 types of certificates. Each type of certificate has own policy identifier (OID 2.5.29.32) according to CPS: Standard certificate [1.2.616.1.113571.1.2.3] Code signing certificate [1.2.616.1.113571.1.2.4] VPN certificate [1.2.616.1.113571.1.2.5] SSL certificate [1.2.616.1.113571.1.2.6] Test certificate [1.2.616.1.113571.1.2.7] ELIXIR certificate [1.2.616.1.113571.1.2.8]
Root Cert URL	for root CA: http://www.elektronicznypodpis.pl/certyfikaty/root_ca.crt for sub CA: http://www.elektronicznypodpis.pl/certyfikaty/trusted_ca.crt
SHA1 Fingerprint	SZAFIR ROOT CA: d3 ee fb cb bc f4 98 67 83 86 26 e2 3b b5 9c a0 1e 30 5d b7 SZAFIR Trusted CA: 23 90 32 95 f3 6a 71 16 39 68 f5 f2 93 01 c7 7f b2 53 86 52

Valid From	SZAFIR ROOT CA: 2011-12-06 SZAFIR Trusted CA: 2011-12-15
Valid To	SZAFIR ROOT CA: 2031-12-06 SZAFIR Trusted CA: 2021-12-15
Certificate Version	X.509 version 3
Certificate Signature Algorithm	sha1RSA
Signing key parameters	RSA keys, the modulus length 2048 bits
Test Website URL (SSL) Example Certificate (non-SSL)	https://ssl.elektronicznypodpis.pl
CRL URL	<p>http://www.elektronicznypodpis.pl/crl/root_ca.crl http://www.elektronicznypodpis.pl/crl/trusted_ca.crl</p> <ul style="list-style-type: none"> The value that nextUpdate is set to in the CRLs for end-entity certificates. <p>Answer: 24 hours</p> <ul style="list-style-type: none"> The sections of your CP/CPS documentation that state the requirements about frequency of updating CRL. <p>Answer: CPS: 4.9.7. Publication Frequency of CRLs</p> <ul style="list-style-type: none"> You must test your CRLs by importing them into the Firefox browser. <p>Answer: Test passed corectly.</p>
OCSP URL	We do not have OCSP
Requested Trust Bits	Requested Trust Bits: Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Validation Type	OV

CA Hierarchy information for each root certificate

CA Hierarchy	<p>Listing and description of all intermediate CAs signed by our root:</p> <p>SZAFIR ROOT CA is on the top of hierarchy, issues only certificates for sub CAs.</p> <p>There is only one subordinate-CA: SZAFIR Trusted CA (internally-operated), which issues 6 types of end-user certificates: Each type of certificate has own policy identifier (OID 2.5.29.32) according to CP:</p> <p>Standard certificate [1.2.616.1.113571.1.2.3] - general purpose end-user certificate type, For protection of information sent electronically, using mainly e-mail, for authorising access to systems, customer authentication in SSL connections. It allows signing and encrypting data in an electronic form and authenticating subscribers.</p> <p>Code signing certificate [1.2.616.1.113571.1.2.4] - For securing codes of programs and confirming authenticity of their origins by affixing</p>
--------------	--

	<p>a signature under this type of code.</p> <p>VPN certificate [1.2.616.1.113571.1.2.5] - For confirming identity of routers in both local and Internet networks. It allows creating virtual private networks by setting up encrypted connections.</p> <p>SSL certificate [1.2.616.1.113571.1.2.6] - For securing www servers and confirming their authenticity. It allows setting up an SSL encrypted connection between servers that have such certificates, and also providing secured logging to customers.</p> <p>Test certificate [1.2.616.1.113571.1.2.7] - For testing co-operation of the certificate with solutions used or developed by a recipient of certification services or a subscriber.</p> <p>ELIXIR certificate [1.2.616.1.113571.1.2.8] - For protecting information sending within ELIXIR and EuroELIXIR systems. This kind of certificates are issued only for Participants of ELIXIR and EuroELIXIR systems.</p>
Externally Operated SubCAs	We do not have any external-operated sub-CAs.
Cross-Signing	Our root certificate has not issued cross-signing certificates and no other root certificates have issued cross-signing certificates for this root certificate.
Technical Constraints	No third-parties (CAs and RAs) can directly cause the issuance of certificates.

Verification Policies and Practices

Policy Documentation	<p>Language(s) that the documents are in: CP: Polish, English CPS: Polish, English Relying Party Agreement: Polish, English</p>
Audits	<p>Audit Type: Audit WebTrust for CAs Auditor: Ernst&Young Auditor Website: www.ey.com URL to Audit Report and Management's Assertions: https://cert.webtrust.org/SealFile?seal=1365&file=pdf</p>
SSL Verification Procedures	<p>URL: http://elektronicznypodpis.pl/files/doc/cps_szafir_trusted_nq_11_20120316_en.pdf Page number: 15-22</p> <p>KIR S.A does not use automatic verification. After identification and authentication the entity, which is conducted by operator, the application goes to another person and next steps of verification are carried out. All applications with high-profile domain names are carried out with special attitude.</p>

<p>Organization Verification Procedures</p>	<p>URL: http://elektronicznypodpis.pl/files/doc/cps_szafir_trusted_nq_11_20120316_en.pdf Page number: 15-22</p> <p>Identification and authentication of entities other than a natural person is the case when data of such entity is included in the data for the certificate for the issuance of which it applies to KIR S.A., or data included in the certificate contains information about such entity, e.g. the name of the Internet domain.</p> <p>Depending on the type of certificate, identification shall be performed on the basis of documents sent by the recipient of certification services or data disclosed in the Agreement and in the order.</p> <p>The manner of confirming such data depends on the type of certificate. For this purpose KIR S.A. may request sending additional documents, check the data of the recipient of certification services in commonly accessible registers and services, obtain a card of signatures of persons authorised to represent the recipient of certification services.</p> <p>Issuance of the certificate may also require a personal meeting of a person authorised to represent a specific entity with an authorised representative of KIR S.A.</p> <p>Wishing to authenticate other data recording which in the certificate a specific entity requests, KIR S.A. may ask for:</p> <ul style="list-style-type: none"> • placing data indicated by KIR S.A. in a target server by the subscriber acting to order of a legal person, which is to verify the rights to the Internet domain; • providing answer to a query sent by KIR S.A. to an e-mail address placing of which in the certificate a legal person demands.
<p>Email Address Verification Procedures</p>	<p>URL: http://elektronicznypodpis.pl/files/doc/cps_szafir_trusted_nq_11_20120316_en.pdf Page number: 15-22</p> <p>Identification and authentication of entities other than a natural person is the case when data of such entity is included in the data for the certificate for the issuance of which it applies to KIR S.A., or data included in the certificate contains information about such entity, e.g. the name of the Internet domain.</p> <p>Depending on the type of certificate, identification shall be performed on the basis of documents sent by the recipient of certification services or data disclosed in the Agreement and in the order.</p> <p>The manner of confirming such data depends on the type of certificate. For this purpose KIR S.A. may request sending additional documents, check the data of the recipient of certification services in commonly accessible registers and services, obtain a card of signatures of persons authorised to represent the recipient of certification services.</p> <p>Issuance of the certificate may also require a personal meeting of a person authorised to represent a specific entity with an authorised representative of KIR S.A.</p> <p>Wishing to authenticate other data recording which in the certificate a specific entity requests, KIR S.A. may ask for:</p> <ul style="list-style-type: none"> • placing data indicated by KIR S.A. in a target server by the subscriber acting to order of a legal person, which is to verify the

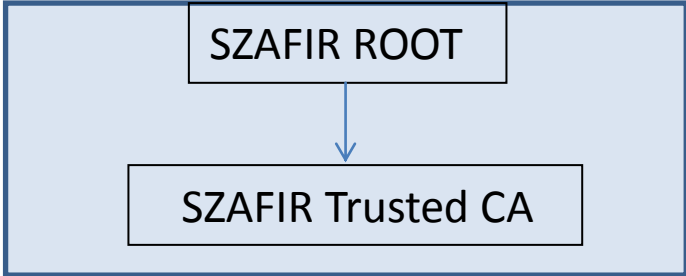
	<p>rights to the Internet domain;</p> <ul style="list-style-type: none"> • providing answer to a query sent by KIR S.A. to an e-mail address placing of which in the certificate a legal person demands.
<p>Code Signing Subscriber Verification Procedures</p>	<p>URL: http://elektronicznypodpis.pl/files/doc/cps_szafir_trusted_nq_11_20120316_en.pdf Page number: 15-22</p> <p>Identification and authentication of entities other than a natural person is the case when data of such entity is included in the data for the certificate for the issuance of which it applies to KIR S.A., or data included in the certificate contains information about such entity, e.g. the name of the Internet domain.</p> <p>Depending on the type of certificate, identification shall be performed on the basis of documents sent by the recipient of certification services or data disclosed in the Agreement and in the order.</p> <p>The manner of confirming such data depends on the type of certificate. For this purpose KIR S.A. may request sending additional documents, check the data of the recipient of certification services in commonly accessible registers and services, obtain a card of signatures of persons authorised to represent the recipient of certification services.</p> <p>Issuance of the certificate may also require a personal meeting of a person authorised to represent a specific entity with an authorised representative of KIR S.A.</p> <p>Wishing to authenticate other data recording which in the certificate a specific entity requests, KIR S.A. may ask for:</p> <ul style="list-style-type: none"> • placing data indicated by KIR S.A. in a target server by the subscriber acting to order of a legal person, which is to verify the rights to the Internet domain; • providing answer to a query sent by KIR S.A. to an e-mail address placing of which in the certificate a legal person demands.
<p>Multi-factor Authentication</p>	<ul style="list-style-type: none"> • For each account that can access the certificate issuance system, do you have the log-in procedure require something in addition to username/password? <p>Answer: Yes, we have smart cards with certificates.</p> <ul style="list-style-type: none"> • Specify the form factor that you use. Examples of multi-factor authentication include smartcards, client certificates, one-time-passwords, and hardware tokens. <p>Answer: Our multi-factor authentication include smartcards with client certificates.</p> <ul style="list-style-type: none"> • This must apply to all accounts that can cause the approval and/or issuance of end-entity certificates, including your RAs and sub-CAs, unless there are technical controls that are implemented and controlled by the CA to restrict certificate issuance through the account to a limited set of pre-approved domains or email addresses. <p>Answer: This apply to all accounts that can cause the approval and/or issuance of end-entity certificates, including our RAs and sub-CAs.</p>

<p>Network Security</p>	<p>Confirm that you have done the following, and will do the following on a regular basis:</p> <ul style="list-style-type: none"> • Check for mis-issuance of certificates, especially high-profile domains. <p>Answer: We do not use automatic verification. After identification and authentication the entity, which is conducted by operator, the application goes to another person and next steps of verification are carried out. All applications with high-profile domain names are carried out with special attitude.</p> <ul style="list-style-type: none"> • Review network infrastructure, monitoring, passwords, etc. for signs of intrusion or weakness. <p>Answer: For provision of the service of certification of keys, hardware and specialist software shall be used that makes up a closed computer system. The system has been executed in the way that satisfies the requirements set forth in the document called CWA 14167-1 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements. Servers and working stations of the system shall be specially prepared to operate in the certification system (hardening of the operating systems) and protected with anti-virus software. Management of the accounts in the system shall be multi-level and performed at the level of the domain/operating system, application of the system managing certificates, and databases. User accounts shall be assigned in accordance with the rules described in the internal documents of KIR S.A.</p> <p>Assessment of security of the computer systems shall be performed on the basis of WebTrust Principles and Criteria for Certification Authorities.</p> <p>Access to the communication and IT system in which certification services are provided shall be protected at the level specified for the provision of certification services that consist in issuance of qualified certificates within the meaning of the Electronic Signature Act and secondary legislation to it.</p> <p>Supervision over security of the computer networks of KIR S.A. is exercised by qualified staff.</p> <ul style="list-style-type: none"> • Ensure Intrusion Detection System and other monitoring software is up-to-date. <p>Answer: Supervision over system development shall be exercised by a Security Inspector. He shall approve the system configuration and the planned changes to the software and hardware. Before it is approved for a production environment, each change shall be tested in a testing environment. After passing rigorous acceptance tests, it may be implemented in the production environment. Any changes in the system shall be recorded in the system documentation and registered in the register of events.</p> <p>Computer hardware and cryptographic modules are selected in such way to be able meet an assumed functionality and security standards. KIR S.A. has extended internal procedures for security management. There is constant monitoring of system security performed at many levels. Examined is the integrity of software, network traffic, configuration of the system and security devices. A system inspection report is regularly prepared. Supervision over system security is exercised by professionals from KIR S.A.</p> <ul style="list-style-type: none"> • Confirm that you will be able to shut down certificate issuance quickly if you are alerted of intrusion.
-------------------------	---

	<p>Compromising of the key of the certification authority is a crisis situation and is part of the BCP. If the private key has been compromised, KIR S.A. shall undertake the following actions:</p> <ol style="list-style-type: none"> 1) revokes the certificate of the certification authority and puts it on CRLs, 2) notifies the certification authority about certificate revocation using available communication channels, 3) generates a new key of the certification authority and new certificates of the subscribers. <p>Detailed actions in the event whereby the key has been compromised are described in the internal procedures of the BCP. In case of disasters and other unpredictable circumstances KIR S.A. has the BCP. Procedures of the BCP strictly define the way of conducting actions necessary for restoring operations. Tests of the BCP procedures are held periodically.</p> <p>KIR S.A. shall have the right to discontinue issuance of certificates. In such event, all subscribers and recipients of certification services shall be informed accordingly with a 90-day notice. Subscribers using certificates, recipients of certification services, and trusted parties shall have no right to make any claims against KIR S.A., provided, however, that KIR S.A. shall still perform its obligations with respect to processing of requests for certificate suspension or revocation and publication of the list of suspended and revoked certificates. Otherwise, recipients of certification services shall have the right to reimbursement of part of the payment for the certificate in proportion of its usage period.</p>
--	---

Response to Mozilla's CA Recommended Practices (https://wiki.mozilla.org/CA:Recommended_Practices)

Publicly Available CP and CPS	<ul style="list-style-type: none"> • The CP/CPS should be publicly available from the CA's official web site. • The format of the CP/CPS document should be PDF or another suitable format for reading documents. CAs should <i>not</i> use Microsoft Word or other formats intended primarily for editable documents. • The CP/CPS should be available in an English version. • The CA should provide references to the CP/CPS sections (e.g., by section number and/or page number) that address the requirements of the Mozilla policy.

CA Hierarchy	 <pre> graph TD A[SZAFIR ROOT] --> B[SZAFIR Trusted CA] </pre> <p>SZAFIR ROOT CA is on the top of hierarchy, issues only certificates for sub CAs.</p> <p>There is only one subordinate-CA: SZAFIR Trusted CA (internally-operated), which issues 6 types of end-user certificates: Each type of certificate has own policy identifier (OID 2.5.29.32) according to CP:</p> <p>Standard certificate [1.2.616.1.113571.1.2.3] - general purpose end-user certificate type, For protection of information sent electronically, using mainly e-mail, for authorising access to systems, customer authentication in SSL connections. It allows signing and encrypting data in an electronic form and authenticating subscribers.</p> <p>Code signing certificate [1.2.616.1.113571.1.2.4] - For securing codes of programs and confirming authenticity of their origins by affixing a signature under this type of code.</p> <p>VPN certificate [1.2.616.1.113571.1.2.5] - For confirming identity of routers in both local and Internet networks. It allows creating virtual private networks by setting up encrypted connections.</p> <p>SSL certificate [1.2.616.1.113571.1.2.6] - For securing www servers and confirming their authenticity. It allows setting up an SSL encrypted connection between servers that have such certificates, and also providing secured logging to customers.</p> <p>Test certificate [1.2.616.1.113571.1.2.7] - For testing co-operation of the certificate with solutions used or developed by a recipient of certification services or a subscriber.</p> <p>ELIXIR certificate [1.2.616.1.113571.1.2.8] - For protecting information sending within ELIXIR and EuroELIXIR systems. This kind of certificates are issued only for Participants of ELIXIR and EuroELIXIR systems.</p>
Audit Criteria	<p>KIR S.A. was evaluated according criteria specified in WebTrust Program for CAs: http://www.cica.ca/resources-and-member-benefits/growing-your-firm/trust-services/item10797.pdf</p> <p>All documents supplied as evidence are publicly available.</p>

	<p>More information about WebTrust Program are available here: http://www.webtrust.org/item64428.aspx</p> <p>URL to Audit Report and Management's Assertions: https://cert.webtrust.org/SealFile?seal=1365&file=pdf</p>
Document Handling of IDNs in CP/CPS	Using of internationalized domain names (IDNs) in certificates is not allowed.
Revocation of Compromised Certificates	CAs should revoke certificates with private keys that are known to be compromised, or for which verification of subscriber information is known to be invalid.
Verifying Domain Name Ownership	<p>Identification and authentication of entities other than a natural person is the case when data of such entity is included in the data for the certificate for the issuance of which it applies to KIR S.A., or data included in the certificate contains information about such entity, e.g. the name of the Internet domain.</p> <p>Depending on the type of certificate, identification shall be performed on the basis of documents sent by the recipient of certification services or data disclosed in the Agreement and in the order.</p> <p>The manner of confirming such data depends on the type of certificate. For this purpose KIR S.A. may request sending additional documents, check the data of the recipient of certification services in commonly accessible registers and services, obtain a card of signatures of persons authorised to represent the recipient of certification services.</p> <p>Issuance of the certificate may also require a personal meeting of a person authorised to represent a specific entity with an authorised representative of KIR S.A.</p> <p>Wishing to authenticate other data recording which in the certificate a specific entity requests, KIR S.A. may ask for:</p> <ul style="list-style-type: none"> • placing data indicated by KIR S.A. in a target server by the subscriber acting to order of a legal person, which is to verify the rights to the Internet domain; • providing answer to a query sent by KIR S.A. to an e-mail address placing of which in the certificate a legal person demands.
Verifying Email Address Control	<p>Identification and authentication of entities other than a natural person is the case when data of such entity is included in the data for the certificate for the issuance of which it applies to KIR S.A., or data included in the certificate contains information about such entity, e.g. the name of the Internet domain.</p> <p>Depending on the type of certificate, identification shall be performed on the basis of documents sent by the recipient of certification services or data disclosed in the Agreement and in the order.</p> <p>The manner of confirming such data depends on the type of certificate. For this purpose KIR S.A. may request sending additional documents, check the data of the recipient of certification services in commonly accessible registers and services, obtain a card of signatures of persons authorised to represent the recipient of certification services.</p> <p>Issuance of the certificate may also require a personal meeting of a person authorised to represent a specific entity with an authorised representative of KIR S.A.</p> <p>Wishing to authenticate other data recording which in the certificate a specific entity requests, KIR S.A. may ask for:</p> <ul style="list-style-type: none"> • placing data indicated by KIR S.A. in a target server by the subscriber acting to order of a legal person, which is to verify the rights to the Internet domain;

	<ul style="list-style-type: none"> providing answer to a query sent by KIR S.A. to an e-mail address placing of which in the certificate a legal person demands.
Verifying Identity of Code Signing Certificate Subscriber	<p>Identification and authentication of entities other than a natural person is the case when data of such entity is included in the data for the certificate for the issuance of which it applies to KIR S.A., or data included in the certificate contains information about such entity, e.g. the name of the Internet domain.</p> <p>Depending on the type of certificate, identification shall be performed on the basis of documents sent by the recipient of certification services or data disclosed in the Agreement and in the order.</p> <p>The manner of confirming such data depends on the type of certificate. For this purpose KIR S.A. may request sending additional documents, check the data of the recipient of certification services in commonly accessible registers and services, obtain a card of signatures of persons authorised to represent the recipient of certification services.</p> <p>Issuance of the certificate may also require a personal meeting of a person authorised to represent a specific entity with an authorised representative of KIR S.A.</p> <p>Wishing to authenticate other data recording which in the certificate a specific entity requests, KIR S.A. may ask for:</p> <ul style="list-style-type: none"> placing data indicated by KIR S.A. in a target server by the subscriber acting to order of a legal person, which is to verify the rights to the Internet domain; providing answer to a query sent by KIR S.A. to an e-mail address placing of which in the certificate a legal person demands.
DNS names go in SAN	If client have other DNS names, we put all the names into the SAN.
Domain owned by a Natural Person	We think that proposal from varga Viktor does not meet RFC criteria.
OCSP	KIR S.A. does not use OCSP.

Response to Mozilla's list of Potentially Problematic Practices (https://wiki.mozilla.org/CA:Problematic_Practices)

Long-lived DV certificates	KIR S.A. issues only OV SSL certificates that have maximum 2 years expiration time.
Wildcard DV SSL certificates	KIR S.A. issues wildcard SSL certificates only to subscribers whose actual identity has been validated with organizational validation (OV).
Email Address Prefixes for DV Certs	KIR S.A. uses an email challenge-response mechanism only as the beginning of the verification process. KIR S.A. uses also placing data indicated by KIR S.A. in a target server by the subscriber acting to order of a legal person, which is to verify the rights to the Internet domain.
Delegation of Domain / Email validation to third parties	In our CA there is no domain/email validation to the third parties.
Issuing end entity certificates directly from roots	KIR S.A. does not issue end entity certificates directly from the root.
Allowing external entities to operate subordinate CAs	In KIR S.A.'s CA there is no subordinate CAs that are operated by external third parties.

Distributing generated private keys in PKCS#12 files	KIR S.A occasionally generates the key pairs for their subscribers but issues them only directly to the subscribers without engaging any other distribution channel.
Certificates referencing hostnames or private IP addresses	KIR S.A does not allow to issue certificates for domains, which are reachable from the public internet.
Issuing SSL Certificates for Internal Domains	KIR S.A. does not allow to issue certificates for domains, which are reachable from the public internet.
OCSP Responses signed by a certificate under a different root	KIR S.A. does not use OCSP.
CRL with critical CDP Extension	It is a problem, that Firefox should solve.
Generic names for CAs	Name of our CA is not generic. It is very unique to allow relatively straightforward identification of the CA.
Lack of Communication With End Users	KIR S.A is very contactable by, and accept and act upon complaints made by, those relying on their assertions of identity. It includes being responsive to members of the general public, including people who have not purchased products from that CA.