Bugzilla ID: 817994
Bugzilla Summary: KIR S.A.'s application for inclusion in Mozilla Root Certificate Program

CAs wishing to have their certificates included in Mozilla products must

1) Comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/)
2) Supply all of the information listed in http://wiki.mozilla.org/CA:Information_checklist.
   a. Review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices
   b. Review the Potentially Problematic Practices at https://wiki.mozilla.org/CA:Problematic_Practices

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 financal institutions e.g. insurance companies.
Inclusion in other browsers	Included in IE - http://social.technet.microsoft.com/wiki/contents/articles/20897.windows-and-windows-phone-8-ssl-root-certificate-program-november-2013.aspx
CA Contact Information	CA Email Alias: certificates@kir.com.pl, 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	SZAFIR ROOT CA

Certificate Issuer Field	CN = SZAFIR ROOT CA
	O = Krajowa Izba Rozliczeniowa S.A.
	C = PL

Certificate Summary	This root currently has one internally-operated intermediate certificate, which issues certificates for SSL, S/MIME, and code signing.
Root Cert URL	http://www.elektronicznypodpis.pl/certyfikaty/root_ca.crt
SHA1 Fingerprint	D3:EE:FB:CB:BC:F4:98:67:83:86:26:E2:3B:B5:9C:A0:1E:30:5D:B7
Valid From	2011-12-06
Valid To	2031-12-06
Certificate Version	3
Certificate Signature Algorithm	SHA-1

Signing key parameters	2048
Test Website URL (SSL)	https://ssl.elektronicznypodpis.pl
CRL URL	http://cdp.elektronicznypodpis.pl/root_ca.crl http://cdp.elektronicznypodpis.pl/trusted_ca_2013.crl
OCSP URL	http://ocsp.elektronicznypodpis.pl The maximum time elapsing from the revocation of an end entity or CA certificate until OCSP responders are updated to reflect that revocation: 1hour The sections of our CP/CPS specifying availability and update requirements for the OCSP service: Page 31, U. 4.9.9; Page 56, U. 7.3.
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Validation Type	OV
EV Policy OID(s)	Not requesting EV treatment.

CA Hierarchy information for each root certificate

CA Hierarchy	There is currently one internally-operated subordinate-CA which issues 6 types of end-user certificates: Each type of certificate has own policy identifiier (OID 2.5.29.32) according to CP: - Standard certificate [1.2.616.1.113571.1.2.3] - For protection of information sent electronically, using mainly e-mail, for authorizing access to systems, customer authentication in SSL connections. It allows signing and encrypting data in an electronic form and authenticating subscribers. - 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] - For testing co-operation of the certificate with solutions used or developed by a recipient of certification services or a subscriber. - 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.
Externally Operated SubCAs	None
Cross-Signing	None
Technical Constraints on Third-party Issuers	Not applicable. No third-parties (CAs and RAs) can directly cause the issuance of certificates.

Verification Policies and Practices

Policy Documentation	Documents are provided in Polish and English CPS: http://www.elektronicznypodpis.pl/files/doc/certification_practice_statement.pdf CP: http://elektronicznypodpis.pl/files/doc/certification_policy.pdf CPS (English): http://elektronicznypodpis.pl/files/doc/cps_szafir_trusted_nq_11_20120316_en.pdf CP (English): http://elektronicznypodpis.pl/files/doc/certification_policy_trusted_nq_20111216_en.pdf

Audits	Audit Type: WebTrust for CAs Auditor: Ernst&Young Auditor Website: www.ey.com Audit Report and Management's Assertions: https://cert.webtrust.org/SealFile?seal=1681&file=pdf (2014.05.05)
Response to CA Communication January 2013	https://wiki.mozilla.org/CA:Communications#January_10.2C_2013 KIR's initial response follows, and I have confirmed completion of the action items: The proposed updates to Mozilla's CA Certificate Policy do not require further change to our CA operations, because our CA operations already comply with the proposed policy. We are working towards compliance with the CA/Browser Forum's Baseline Requirements, but we need to complete: · including CRL Distribution Point or OCSP URI in the intermediate certificate (plan to be completed: by the end of the year 2013) · implementation of OCSP and including OCSP URI in the AIA End-entity certs (plan to be completed: by the end of the year 2013) · Commitment to Comply with the CA/Browser Forum Baseline Requirements (plan to be completed: June 2013) · changing Certification Policy in case of issuing test certificates (plan to be completed: June 2013).
Response to CA Communication July 2013	https://wiki.mozilla.org/CA:Communications#July_30.2C_2013 KIR's response: Action #1 (BR #11.1.4, new gTLD domains) -- A Action #2 (Knowing or intentional mis-issuance) -- acknowledged Action #3 (Spreadsheet of included root certs) – New links provided, spreadsheet updated. Action #4 (Complete response to previous Communication) - A
Baseline Requirements (SSL)	https://cert.webtrust.org/SealFile?seal=1681&file=pdf CPS section 1.1: KIR S.A. provides certification services in compliance with the requirements of the current version of the Baseline Requirements for the Issuance and Management of Publicly- Trusted Certificates published at www.cabforum.org. In the event of any discrepancies between the CSP and the said document, the document shall prevail over the CSP.
Organization Verification Procedures	CPS section 3.2: Prior to the issuance of the first certificate for a specific subscriber, the recipient of certification services shall execute an Agreement and deliver to KIR S.A. an order containing data necessary for certificate preparation. An order for the certificate may also be submitted via a form available at the website of KIR S.A. The first certificate may be issued together with a pair of keys or to a public key from a pair generated by the subscriber. In the second case, the subscriber should prove the fact of having a private key in accordance with the guidance of sub-Clause 3.2.1. To receive a certificate it is necessary for the subscriber who is a natural person or an authorised representative of the recipient of certification services to present: 1) an identification card (or its photocopy depending on the type of certificate); 2) documents confirming rights to the domain (optionally, relative to the certificate type); 3) a file with the certificate request (if the pair of keys is generated individually by the subscriber). CPS section 3.2.2: 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. 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. 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. 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.
SSL Verification Procedures	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. CPS section 3.2.2: Wishing to authenticate other data recording which in the certificate a specific entity requests, KIR S.A. may ask for: 1) 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; 2) 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. CP section 2.4: In the process of issuing this type of certificates the operator KIR S.A. shall verify the subscriber's identity and its right to obtain a certificate. The process may also include verification, whether the server or domain are held by the recipient of certification services.
Email Address Verification Procedures	CPS section 3.2.2 (see above). – Ownership/control is demonstrated by an email challenge-response mechanism. CP section 2.1 (Standard certificate): In the process of issuing this type of certificates the operator KIR S.A. shall verify the subscriber's identity and the right to obtain such certificate. The certificate is delivered to the subscriber most often with a pair of keys generated on a carrier defined by the subscriber. Data included in the certificate allows identifying the subscriber that uses the certificate.
Code Signing Subscriber Verification Procedures	CP section 2.2: In the process of issuing this type of certificates the operator KIR S.A. shall verify the subscriber's identity and the right to obtain such certificate and shall confirm reliability of the data entered into the certificate.
Test Certificates	CP section 2.5, Test certificate: These certificates are used for checking co-operation with the system or the subscriber's IT solution. In the process of issuing this type of certificates the operator KIR S.A. verify the subscriber's right to obtain such certificate. In case, when test certificate is to serve to examine the possibility of setting up secure connections, then process includes also verification, if www server or domain are at the disposal of recipient of certification services.
Multi-factor Authentication	Confirm that multi-factor authentication is required for all accounts capable of directly causing certificate issuance. Answer: Yes, we have smart cards with certificates. Our multi-factor authentication includes smartcards with client certificates. This applies to all accounts that can cause the approval and/or issuance of end-entity certificates, including our RAs and sub-CAs.
Network Security	CPS sections 5 and 6

	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. 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. Assessment of security of the computer systems shall be performed on the basis of WebTrust Principles and Criteria for Certification Authorities. 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. 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. 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. Anwer: 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: 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. 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.

	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.

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

Publicly Available CP and CPS	Yes, see above.
CA Hierarchy	Yes, see above.
Audit Criteria	Yes, see above.
Document Handling of IDNs in CP/CPS	Using of internationalized domain names (IDNs) in certificates is not allowed.
Revocation of Compromised Certificates	
Verifying Domain Name Ownership	Yes, see above.
Verifying Email Address Control	Yes, see above.
Verifying Identity of Code Signing Certificate Subscriber	Yes, see above.
DNS names go in SAN	If client have other DNS names, we put all the names into the SAN.
OCSP	Yes, see above.

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	No
Issuing end entity certificates directly from roots	No
Allowing external entities to operate subordinate CAs	No
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.' OCSP Responses are signed by a certificate under a proper root (SZAFIR ROOT CA).
CRL with critical CIDP Extension	CRL imported into Firefox browser without error.
Generic names for CAs	No.
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.