Print this page

Mozilla - CA Program

Case Information

Case Number	00000026	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	Krajowa Izba Rozliczeniowa S.A. (KIR)	**Request Status**	Approved, Pending Inclusion

Additional Case Information

Subject	Add Krajowa Izba Rozliczeniowa S.A. CA and Root	**Case Reason**	New Owner/Root inclusion requested

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org/show_bug.cgi?id=817994

General information about CA's associated organization

CA Email Alias 1	certificates@kir.com.pl		
CA Email Alias 2			
Company Website	http://www.kir.com.pl/	**Verified?**	Verified
Organizational Type	Private Corporation	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	Poland	**Verified?**	Verified
Primary 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.	**Verified?**	Verified
Impact to Mozilla Users	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.	**Verified?**	Verified

Response to Mozilla's list of Recommended Practices

Recommended Practices	https://wiki.mozilla.org/CA:Recommended_Practices#CA_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's list of Recommended Practices, and confirm that we follow those

			practices, with exceptions and clarifications noted in the text box below.
CA's Response to Recommended Practices	Yes to all. * Using of internationalized domain names (IDNs) in certificates is not allowed. * If client have other DNS names, we put all the names into the SAN.	**Verified?**	Verified

Response to Mozilla's list of Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices	**Problematic Practices Statement**	I have reviewed Mozilla's list of Potentially Problematic Practices, and confirm that we do not do those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Problematic Practices	* CPS section 6.3.2: maximum validity for SSL certs is 3 years, excluding ELIXIR certs for which operational period is maximum 2 years. * KIR S.A. issues wildcard SSL certificates only to subscribers whose actual identity has been validated with organizational validation (OV). * 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. * 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. * KIR S.A does not allow to issue certificates for domains, which are reachable from the public internet. * CPS section 7.1.1: Beginning from 1 January 2016 all certificates issued by KIR S.A shall have an SHA-256 function.	**Verified?**	Verified

Root Case Record # 1

Root Case Information

Root Certificate Name	SZAFIR ROOT CA2	**Root Case No**	R00000030
Request Status	Approved, Pending Inclusion	**Case Number**	00000026

Additional Root Case Information

Subject	Include SZAFIR ROOT CA2 root

Technical Information about Root Certificate

O From Issuer Field	Krajowa Izba Rozliczeniowa S.A.	**Verified?**	Verified
OU From Issuer Field		**Verified?**	Verified
Certificate Summary	This root currently has one internally-operated intermediate certificate, which issues certificates for SSL, S/MIME, and code signing.	**Verified?**	Verified
Root Certificate Download URL	http://www.elektronicznypodpis.pl/certyfikaty/root_ca2.crt	**Verified?**	Verified

Valid From	2015 Oct 19	**Verified?**	Verified
Valid To	2035 Oct 19	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	SHA-256	**Verified?**	Verified
Signing Key Parameters	2048	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	https://ssl.elektronicznypodpis.pl/	**Verified?**	Verified
CRL URL(s)	http://cdp.elektronicznypodpis.pl/root_ca2.crl http://cdp.elektronicznypodpis.pl/trusted_ca2.crl	**Verified?**	Verified
OCSP URL(s)	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.	**Verified?**	Verified
Revocation Tested	https://certificate.revocationcheck.com/ssl.elektronicznypodpis.pl lists the error: Response is not yet valid in the OCSP Get and Post sections	**Verified?**	Error
Trust Bits	Email; Websites	**Verified?**	Verified
SSL Validation Type	OV	**Verified?**	Verified
EV Policy OID(s)	Not EV	**Verified?**	Not Applicable
EV Tested		**Verified?**	Not Applicable
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	E2:52:FA:95:3F:ED:DB:24:60:BD:6E:28:F3:9C:CC:CF:5E:B3:3F:DE	**Verified?**	Verified
SHA-256 Fingerprint	A1:33:9D:33:28:1A:0B:56:E5:57:D3:D3:2B:1C:E7:F9:36:7E:B0:94:BD:5F:A7:2A:7E:50:04:C8:DE:D7:CA:FE	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	There is currently one internally-operated subCA which issues 6 types of end-user certificates: - Standard -- e-mail, for authorizing access to systems, signing and encrypting data in an electronic forms and authenticating subscribers. - Code signing - VPN - SSL - Test - ELIXIR -- We will start to issue all Elixir certs including the EKU extension with	**Verified?**	Verified

	value id-kp-clientAuth from the 15th of February. We will update our CPS to reflect this. It will be valid from the same date.		
Externally Operated SubCAs	None	**Verified?**	Verified
Cross Signing	None	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	Not applicable. No third-parties (CAs and RAs) can directly cause the issuance of certificates.	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Documents are provided in Polish and English.	**Verified?**	Verified
CA Document Repository	Polish: http://www.elektronicznypodpis.pl/informacje/podstawy-prawne/ English: http://eng.elektronicznypodpis.pl/en/information/documents-and-agreements	**Verified?**	Verified
CP Doc Language	English		
CP	http://elektronicznypodpis.pl/files/doc/certification_policy.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	http://www.elektronicznypodpis.pl/files/doc/certification_practice_statement.pdf	**Verified?**	Verified
Other Relevant Documents		**Verified?**	Not Applicable
Auditor Name	EY	**Verified?**	Verified
Auditor Website	http://www.ey.com/	**Verified?**	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	**Verified?**	Verified
Standard Audit	https://cert.webtrust.org/SealFile?seal=1845&file=pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	3/18/2015	**Verified?**	Verified
BR Audit	https://cert.webtrust.org/SealFile?seal=1845&file=pdf	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	3/18/2015	**Verified?**	Verified
EV Audit		**Verified?**	Not Applicable
EV Audit Type		**Verified?**	Not Applicable
EV Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	CPS section 1.1	**Verified?**	Verified
SSL Verification Procedures	CPS section 3.2.2: If an SSL certificate and a test certificate is to contain a domain name, checking shall include if a recipient of certification services has the	**Verified?**	Verified

	right to use the domain name and if the domain remains under its control. Verification performed by KIR S.A. shall comprise: - checking in publicly available WHOIS services or directly with entities registering domains, if a recipient of certification services is registered as a domain owner or has the right to use the domain name; - checking, if a response has been sent to an e-mail sent by KIR to the domain administrator to an e-mail address of the administrator domain containing webmaster, admin, administrator, hostmaster, postmster before @domena or an e-mail address indicated as the address for contacts for a specific domain in the WHOIS service or the register of domains; - checking, if verification data indicated by KIR S.A. has been placed on a server or in a record such as TXT in DNS; - in case of Wildcard Certificates checking if in the “public suffix list” (PSL) register http://publicsuffix.org/ (PSL), the sign “*” is not put in the first place on the left-hand side of the suffix of gTLD domains delegated by ICANN. KIR S.A. may issue a Wildcard Certificate for gTLD domains, if the subscriber properly proves its right to manage the entire space of names under the gTLD domain.		
EV SSL Verification Procedures	Not requesting EV treatment	**Verified?**	Not Applicable
Organization Verification Procedures	CPS section 3.2	**Verified?**	Verified
Email Address Verification Procedures	Ownership/control of email address to be included in the certificate is demonstrated via an email challenge-response mechanism. CPS section 3.2.2: If a certificate is to provide for security of electronic mail, verification of the electronic mail address shall be done. Verification shall consist in checking if an electronic mail address indicated in the order belongs to the subscriber. Checking may be done by confirming that the subscriber has collected authentication data sent to an electronic mail address given in the order. Checking is to determine that the e-mail address is legally used by the subscriber.	**Verified?**	Verified
Code Signing Subscriber Verification Pro	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.	**Verified?**	Verified
Multi-Factor Authentication	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.	**Verified?**	Verified

Network Security	CPS sections 5 and 6	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	https://bugzilla.mozilla.org/show_bug.cgi?id=817994	**Verified?**	Verified