

Bugzilla ID: 817994

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

Technical information about each root certificate

CRL URL	We issued new intermediate certificate with CRL Distribution Point and OCSP URI. The CRL Distribution Point: http://cdp.elektronicznypodpis.pl/trusted_ca_2013.crl
OCSP URL (Required now)	<p>The OCSP URI that is in the AIA of your subscriber certificates: http://ocsp.elektronicznypodpis.pl</p> <p>The maximum time elapsing from the revocation of an end entity or CA certificate until OCSP responders are updated to reflect that revocation: 1hour</p> <p>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.</p> <p>We tested that our OCSP service is compatible with the Firefox browser.</p>

Verification Policies and Practices

Response to CA Communication	CA Communications (January 10, 2013)					Comments
	Action #1 Policy Update Readiness	Action #2 Baseline Requirements Readiness	Action #3 Scan Certificate Database	Action # 4 Stop including reserved IP address in SSL certificates	Action #5 URL to Test Website	
	A	A	B*	A	Provided	<p>*There are end-entity certificates with RSA key sizes smaller than 2048 bits expire later than December 2013.</p> <p>They are being issued only to special group of users - participants in ELIXIR and EuroELIXIR systems operating by KIR S.A for protecting information transmitted within these systems. These certificates will be replaced by December 2015.</p>

CA Communications (July 13, 2013)						
	Action #1 BR #11.1.4, new gTLD domains	Action #2 Knowing or intentional mis-issuance	Action #3 Spreadsheet of included root certs	Action #4 Complete response to previous Communication	Item #5 Revoked Intermediate Certs (action requested, not required at this time)	Comments
	A	acknowledged	We have added more user friendly links to CP and CPS: http://www.elektronicznypodpis.pl/files/doc/certification_practice_statement.pdf http://elektronicznypodpis.pl/files/doc/certification_policy.pdf	A		
Baseline Requirements (SSL)	"Commitment to Comply" with the CA/Browser Forum Baseline Requirements may be found in CPS (page 9, U. 1.1). In our next audit we will include verification of compliance with the CA/Browser Forum Baseline Requirements.					
Test Certificates	We changed procedures of issuing test SSL and S/MIME certificates and now in the process of issuing these types of certificates the operator KIR S.A. shall verify the subscriber's identity and the right to obtain such certificate.					

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

OCSP	Yes, see above
------	----------------

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

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).
---	--