CRL URL	No CRL Distribution Point or OCSP URI in the intermediate certificate. Comment #5: We placed in our Sub CA certificate only the link to CPS. In this document there is the address for CRL. Among UE countries, there is currently an ongoing discussion about the new regulation on electronic identification and trust services for electronic transaction in the internal market. They are discussing different way of certificate validation and that is why we decided not to point CRL address in subCA certificates. Please see Appendix B of the CA/Browser Forum's Baseline Requirements (https://www.cabforum.org/documents.html). "(2) Subordinate CA Certificate ... B. cRLDistributionPoints This extension MUST be present and MUST NOT be marked critical. It MUST contain the HTTP URL of the CA's CRL service." http://www.elektronicznypodpis.pl/crl/trusted_ca.crl (NextUpdate: 1 day) CPS section 4.9.7: CRLs for certificates issued by the operational certification authority SZAFIR Trusted CA shall be published always after certificate suspension or revocation, however, not less frequently than every 24 hours. **KIR's answer:** We understand this requirement but fullfiling it is complex, because we need to generate new intermediate certificate. It will be possible by the end of the year 2013. Could you please confirm that with this commitment it will be possible to proceed without any delays in Mozilla Root Certificate Program?
OCSP URL (Required now)	End-entity certs need to have the OCSP URI in the AIA. Comment #5: We did not implement OCSP, as it is not very popular now. We are monitoring questions from our current clients and if they are interested in such services then we will implement it. OCSP is required for EV enablement and we do not issue such certificates. Please see Appendix B of the CA/Browser Forum's Baseline Requirements (https://www.cabforum.org/documents.html). "(2) Subordinate CA Certificate ... C. authorityInformationAccess With the exception of stapling, which is noted below, this extension MUST be present. It MUST NOT be marked critical, and it MUST contain the HTTP URL of the Issuing CA's OCSP responder" And "(3) Subscriber Certificate ... C. authorityInformationAccess With the exception of stapling, which is noted below, this extension MUST be present. It MUST NOT be marked critical, and it MUST contain the HTTP URL of the Issuing CA's OCSP responder" **KIR's answer:**

	We understand this requirement. Implementation of OCSP takes time and it will be done by the end of the year 2013.
Response to CA Communication	Please respond to the action items listed in the recent CA Communication: https://wiki.mozilla.org/CA:Communications#January_10.2C_2013 **KIR's answer:** 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).
Baseline Requirements (SSL)	The document(s) and section number(s) where the "Commitment to Comply" with the CA/Browser Forum Baseline Requirements may be found, as per BR #8.3. (https://www.cabforum.org/documents.html) Audits performed after January 2013 need to include verification of compliance with the CA/Browser Forum Baseline Requirements if SSL certificates may be issued within the CA hierarchy, and the audit statement shall indicate the results. Comment #5: We have provided you with information about our CA on 4th December 2012. Our audit was performed in June 2012 so it was impossible to include this requirement in it. We checked CPS and CP issued by another Polish CA which you have approved as valid at that time and no such statement has been found there. If you are referring to Unizeto Certum, they have indicated that they are working to become compliant with the CA/Browser Forum's BRs, and have committed: OCSP requirements for end user certificates will be fulfilled by July 2013, some changes in CPS are also required, and will be done in the middle of April. https://wiki.mozilla.org/CA:Communications#January_2013_Responses I understand if you also need more time to become compliant with the BRs, but they are now a required part of Mozilla's policy. **KIR's answer:** We understand this requirement. We will put the „Commitment to Comply" in our CPS by June 2013.
Test Certificates	CP section 2.5: In the process of issuing this type of certificates the operator KIR S.A. shall not verify the subscriber's identity and its right to obtain such certificate. Data included in the certificate does not allow identification of the subscriber using the

	certificate. What prevents someone from getting a test SSL certificate for a website they don’t own/control, or an S/MIME certificate for an email address they don't own/control? Comment #5: We would like to emphasise that Data included in the certificate does not allow identification of the subscriber using the certificate. The certificate has OID pointed on the test certificates. So if the usage of certificates is to be implemented properly, such certificates should not be used to user’s identification. During the WebTrust audit there was no problem with the test certificates applied in such way. Sorry, I do not understand your answer. What domain names can be included in a test SSL certificate? I am trying to understand how a test SSL certificate with no verification performed is not capable of being used maliciously. And why does the test SSL cert have to chain up to a publicly trusted root cert? **KIR’s answer:** Sorry for misundrestanding. We will change our Certification Policy in case of issuing test certificates. Full verification of any data will be included in this documents and in practise. It will be done by June 2013. We would like to fullfil any requirements you recognize as important.