Bugzilla ID: 480966
Bugzilla Summary: Netlock Root CA rollover request

CAs wishing to have their certificates included in Mozilla products must comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/) and must supply the information necessary to determine whether or not the policy's requirements have been satisfied, as per http://wiki.mozilla.org/CA:Information_checklist.

General Information	**Data**
CA Name	NetLock
Website URL (English version)	http://www.netlock.hu/USEREN/index.html
Organizational type. (E.g., whether the CA is operated by a private or public corporation, government agency, academic institution or consortium, NGO, etc.)	NetLock Ltd. developed into an independent organisation in October 1996.
Primary market / customer base. (Which types of customers does the CA serve? Are there particular vertical market segments in which it operates? Does it focus its activities on a particular country or other geographic region?)	NetLock Ltd. is a qualified Certificate Authority in Hungary that issues certificates to organizations and individuals.

For Each Root CA whose certificate is to be included in Mozilla (or whose metadata is to be modified)

Info Needed	**Data**
Certificate Name	NetLock Arany (Class Gold) Főtanúsítvány
Cert summary / comments	NetLock currently has four separate root CAs included in NSS. The redesigned equivalent of these existing roots will be created under this new root. The subordinate CAs of the new root will be at minimum a qualified and a non-qualified root. There are currently two externally-operated subordinate CAs of the existing Class B root, MKB (Hungarian Trade Bank) and MNB (National Bank of Hungary). MKB and MNB will be part of the new CA chain, but there is no decision yet of the level of inclusion. They will probably be under the non-qualified subordinate CA.
The root CA certificate URL Download into FireFox and verify	https://bugzilla.mozilla.org/attachment.cgi?id=365241
SHA-1 fingerprint.	06:08:3f:59:3f:15:a1:04:a0:69:a4:6b:a9:03:d0:06:b7:97:09:91
Valid from	2008-12-11

Valid to	2028-12-06
Cert Version	3
Modulus length	2048
CRL - URL - update frequency for end-entity certificates	Not yet available. Comment #8: I don’t have concrete time about it, but will be available in the same form like actual roots and its crls. CPS section 4.10.1: Validity of the lists is at most twenty-four (24) hours.
OCSP Responder URL	Not yet available. CPS section 4.9.5, Revocation Request Grace Period The revocation steps are continous steps without delay. The status of the revoked certificate gets into the certificate database immediately, so the online certificate status check is possible. After a Certificate state change, there will be a new CRL issued, in one (1) hour, and this CRL holds the changed state of the revoked certificate. NetLock accepts continuously the revocation applications demanding human intervention and starts their processing immediately. After starting the processing and making decision on the change in certificate status, NetLock refreshes the certificate status data base without delay, if necessary. Period of processing the revocation applications demanding human intervention is at most three (3) hours. If during this period NetLock cannot make certain of the authenticity of the revocation/suspension application by no fault of its own, it refuses to deal with the application further on.
List or description of subordinate CAs operated by the CA organization associated with the root CA.	The roots that are currently in NSS are: 1. NetLock Minositett Kozjegyzoi (Class QA) Tanusitvanykiado 2. NetLock Kozjegyzoi (Class A) Tanusitvanykiado 3. NetLock Uzleti (Class B) Tanusitvanykiado a. The current Class B CA has 2 sub-CAs, MKB (Hungarian Trade Bank) and MNB (National Bank of Hungary). 4. NetLock Expressz (Class C) Tanusitvanykiado The redesigned equivalent of these existing roots will be created under the new root. The new root, NetLock Arany (Class Gold) Főtanúsítvány, is an independent, self-signed root. The subordinate CAs of the new root will be at minimum a qualified and a non qualified root, MNB and MKB will be the part of the chain, but there is no decision yet of the level of inclusion. They will probably be under the non qualified subordinate CA.

For subordinate CAs operated by third parties, if any: General description of the types of third-party subordinates that exist, and what the general legal/technical arrangements are by which those subordinates are authorized, controlled, and audited.	Will create a separate document to summarize the information about the subordinate CAs as per https://wiki.mozilla.org/CA:SubordinateCA_checklist The Class B root that is currently included in NSS will be rolled-over to a new sub-CA that is subordinate to this root. As such, this root will have two sub-Cas that are operated by third parties. They are: MKB (Hungarian Trade Bank) This sub-CA is used for internal certificate issuance, only for workers of the MKB bank. It issues only signer and encryption certificates for the workers. MNB (National Bank of Hungary). This sub-CA issues 1. Signer and encryption certificates for workers. 2. Signer and encryption certificates for third party contractual partners of the bank. The MNB is the Central Bank of Hungary, and their partners should provide for them periodical reports. 3. server certificates for internal use on servers (only for internal server authentication) Controls: 4. Contract between CA and third party 5. Configuration of issuing server 6. CPS 7. They can't create subordinates, controlled by PATHLEN 8. CA audits of subordinates 9. Third party audits made by the governmental agency NHH (National Communications Agency). 10. Frequency of audits: Yearly.
List any other root CAs that have issued cross-signing certificates for this root CA	None
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing
If SSL certificates are issued within the hierarchy rooted at this root CA certificate: • Whether or not the domain name referenced in the	IV/OV CPS: • Section 3.2.2, Authentication of Organization Identity • Section 3.2.3, Authentication of Individual Identity

certificate is verified to be owned/controlled by the certificate subscriber. (DV) • Whether or not the value of the Organization attribute is verified to be that associated with the certificate subscriber in addition to verifying the domain name. (OV)	• NetLock verifies the identity of organizations as described in the Table in Section **Error! Reference source not found.** • Checking the identity, comparing the photo in the identity document to the Applicant; comparing the signature in the identity document with that on the Service Agreement, Personal presence before Netlock is needed. Entitled to perform by the decision of the end user: Central Registration Authority or Mobile Registration Unit or registration and delivery delegate • NetLock shall reject a certificate application if: identity of the natural person and/or organization cannot be verified without doubt
EV policy OID(s)	Not requesting EV-enablement at current time. EV certificate issuing is planned. Comment #8: 5)I did not find reference to Extended Validation Criteria in the CPS. At first do the rollover, and then later, change the settings to the EV.
Example certificate(s) issued within the hierarchy rooted at this root, including the full certificate chain(s) where applicable. • For SSL certificates this should also include URLs of one or more web servers using the certificate(s). • There should be at least one example certificate for each of the major types of certificates issued, e.g., email vs. SSL vs. code signing, or EV vs. OS vs. DV. • Note: mainly interested in SSL, so OK if no email	User certificate issued for testing purpose with this root. https://bugzilla.mozilla.org/attachment.cgi?id=364928 The root will not issue this type of certificate later, the root will be used only for intermediate roots.

example.	
CP/CPS	CPS in English: https://bugzilla.mozilla.org/attachment.cgi?id=364923 Practice Statements and Terms of Agreements in Hungarian: http://www.netlock.hu/USEREN/html/dok.html Translations into English: Non-qualified certificate CPS actual version (for signing and timestamping) https://bugzilla.mozilla.org/attachment.cgi?id=366607 For OV, IV the paractice can be found in the CPS_NQ_080206. Non-qualified certificate CRL and OCSP profile definitions https://bugzilla.mozilla.org/attachment.cgi?id=366794 Domain validation in server certificate issuance https://bugzilla.mozilla.org/attachment.cgi?id=366795 This is a small still valid part of the 2003-02-25 dated Certificate issuance practice statement. Because the verifications are overdefined by the CPS_NQ_080206, it has only this small block that is still valid. Its on the server certificate issuance domain verification. Comment #27: In Hungary the Electronic Signature Law controls only the certificates with signature and timestamping purpose. Later, the NCA forces us, to separate the CPS for the purposes, which are under the control of this law, and to others. The older CPS is still valid, for non signature and timestamp purpose. Because the new signature specific CPS overwrites the verification for natural persons and organizations, only the server identification is valid. We are working on the unified version of the CPSs, but now I can only send you the actual valid CPSs. Comment #28: The old CPS is still valid for non-signature and non-timestamp specific purpose...
AUDIT	Audit Type: ETSI TS 101 456, ETSI 102 042 Auditor: National Communications Authority, Hungary Auditor Website: http://webold.nhh.hu/esign/setLanguageAction.do?lang=en Statement of audit conformance in English: https://bugzilla.mozilla.org/attachment.cgi?id=365687

	Statement of National Communications Authority that Netlock is a Qualified Service Provider: http://webold.nhh.hu/esign/szolgReszlet/init.do?tipus=mi&azon=12201521-2-41 The NCA URL contains “webold” because the website is under redesign. Date of Last audit: May 5, 2008 Date of Next audit: Spring, 2009 Auditor contact info: Dr. Nóra Sylvester sylvester.nora@nhh.hu Directorate of Informatics Regulation National Communication Authority

Review CPS sections dealing with subscriber verification
(section 7 of http://www.mozilla.org/projects/security/certs/policy/)

- Verify the domain referenced in an SSL cert is owned/controlled by the subscriber. In addition to verification of subscriber’s legal identity.
    - https://bugzilla.mozilla.org/attachment.cgi?id=366795 -- 3.2.7, Server identification
        - With this verification the owner of the server should be identified. This is the only possible way to do this. This was made by Registration staff.
            - The domain name should be queried through public and verified name servers. The owner of that domain who is authorized to request a certificate for that DNS name
        - The verification was successful, if the owner of domain name is the same as the requestor. If they are not same, Netlock refuses the request.
- Verify the email account associated with the email address in the cert is owned by the subscriber. In addition to verification of subscriber’s legal identity.
    - CPS section 4.2.2:
        - Automated confirmations, checking of the e-mail address (if the Subject has any).
        - NetLock confirms the certificate application in an automated reply. The Applicant shall send a reply to the confirmation
        - Entitled to perform: natural person, applying employee
    - From NetLock: same applicable on qualified and non qualified except the SSCD related things
- Verify identity info in code signing certs is that of subscriber
    - From NetLock:
        - Code Signing certificates are handled like signer certificates and they are issued from the QA root only, of-course the profile of the code signing is slightly different than the other qualified signer.

        - The requestor of the code signing certificate is evaluated fully through the qualified CPS, its certificate is handled like a signer certificate, exclusively given only on SSCD device.
        - Regarding the agreement between MS and Netlock, it is possible to request the revocation of that code signing certificate from third party, and this revocation after the needed check will be done. Of-course, the code signing profile has the CodeSign EKU.
- Make sure it’s clear which checks are done for which context (cert usage)
- All documents supplied as evidence should be publicly available and must be addressed in any audit. Any substantial omissions submitted afterwards may need to be confirmed by auditor, at Mozilla's discretion.

Flag Problematic Practices (COMPLETE)
(http://wiki.mozilla.org/CA:Problematic_Practices)

- Long-lived DV certificates
    - Certs are OV.
    - CPS Section 7.1.1: Validity of the end user private key corresponds to that of the related certificate, but maximum 2 years, renewing the certificate with same key this maximum will be 4 years. The public key is valid until it is secure cryptographically.
- Wildcard DV SSL certificates
    - Certs are IV/OV.
    - Wildcard SSL certificates are validated with IV/OV too.
- Delegation of Domain / Email validation to third parties
    - Domain and email validation is done internally, by the Central Registration Authority.
- Issuing end entity certificates directly from roots
    - No, will issue via subordinate CAs.
    - This is one of the goals of the rollover. At now the actual way is this, after the rollover, we switch to the offline root, subordinate CA combo. At the start of the actual roots there was no criteria like this.
- Allowing external entities to operate unconstrained subordinate CAs
    - External entities are allowed to operate subordinate CAs, as described above.
    - At this time, MNB and MKB subordinated external CA is constrained by the CA:TRUE, pathlen:0 constraint. Systems are configured and maintained by Netlock.
- Distributing generated private keys in PKCS#12 files
    - There is no distribution of private keys in PKCS#12 except personal encryption certificates.
    - As a backup, encryption certificates requested on signature device are given on CD to the user, if she/he lost his device, it is possible with the PKCS#12 backup, to open encrypted mails. Now key recovery is possible trough online system but only for these personal encryption certificates.
    - CPS Section 7.1.1:

        - Key pair generation shall be carried out by the End User himself/herself or − in case of signing device services − NetLock. Key pair generation and storage for End Users is permitted exclusively on SSCD. For generating Signature Creating Data, NetLock shall use SSCD or cryptographic hardware device certified according to the legislative provisions.
        - NetLock applies multi-person control or adequate technical protection when generating and managing private keys.
    - CPS Section 7.1.2:
        - Since all the key pairs of NetLock are generated on-site (see Section **Error! Reference source not found.**), they shall be transmitted to nowhere.
        - The signing private keys of the End Users shall not be transmitted if they are generated by the Subject himself/herself. When the end user key pair is generated by NetLock within the frame of Signing Device Services, it delivers the device to the Subject in a direct and secure way.
- Certificates referencing hostnames or private IP addresses
    - There is no certificate issued to domains without FQDN.
- OCSP Responses signed by a certificate under a different root
    - Comment #19: root CA will use its OCSP responder, and subordinate CAs will use their responder too.
    - In the current architecture only CDP field is included into the certificate. After the rollover there will be AIA fields too, and this AIA field will be compatible with this option. Certificates with OCSP AIA will have public access and will have OCSP responder issued with the same root as the certificate.
- CRL with critical CIDP Extension
    - CRL does not have CIDP extension, and they are not and not will be partitioned.

Verify Audits (COMPLETE)
(Sections 8, 9, and 10 of http://www.mozilla.org/projects/security/certs/policy/)

- Validate contact info in report, call to verify that they did indeed issue this report.
    - NetLock is listed on NHH Qualified Service Providers website.
- For EV CA’s, verify current WebTrust EV Audit done.
    - Not requesting EV-enablement at this time.
- Review Audit to flag any issues noted in the report
    - No issues noted in report.