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	NetLock Ltd. developed into an independent organisation in October 1996.
Primary market / customer base.	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 new root will sign 7 internally-operated subordinate CAs. Two of those subordinate CAs will sign sub-CAs that will be externally-operated by MKB (Hungarian Trade Bank) and MNB (National Bank of Hungary).
The root CA certificate URL	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
Test Website	https://www.schalamonek.hu/ The website cert is signed by CN = NetLock Üzleti (Class B) Tanúsítványkiadó Which is signed by CN = NetLock Arany (Class Gold) Főtanúsítvány
CRL URL update frequency for end-entity certificates	http://crl1.netlock.hu/index.cgi?crl=gold CLASS B LEGAL: http://crl1.netlock.hu/index.cgi?crl=cblca CLASS B: http://crl1.netlock.hu/index.cgi?crl=cbca CPS section 4.10.1: Validity of the lists is at most twenty-four (24) hours.

OCSP Responder URL	http://ocsp1.netlock.hu/gold.cgi CLASS B LEGAL: http://ocsp1.netlock.hu/cblca.cgi CLASS B: http://ocsp1.netlock.hu/cbca.cgi

List or description of subordinate CAs operated by the CA organization associated with the root CA.	CA Hierarchy: https://bug480966.bugzilla.mozilla.org/attachment.cgi?id=374930
	Dark Blue color = ready/usable, Light Blue = planned
	
	The new root, NetLock Arany (Class Gold) Főtanúsítvány, is an independent, self-signed root with the following subordinate CAs.
	• Qualified subCA (QA) – only signer certificates
	• Non-Qualified subCA (A Eat. – Legal) – only signer certificates
	• Non-Qualified subCA (B Eat. – Legal) – only signer certificates
	  o MKB subCA Legal
	  o MNB subCA Legal
	  o End user signer certificate
	• Non-Qualified subCA (C Eat. – Legal) – only signer certificates
	• Non-Qualified subCA (A) – SSL, encryption, and authentication certificates
	• Non-Qualified subCA (B) – SSL, encryption, and authentication certificates.
	  o MKB subCA
	  o MNB subCA
	  o End user certificate (non-signer)
	• Non-Qualified subCA (C) – SSL, encryption, and authentication certificates
	
	The A Eat.-Legal, B Eat.-Legal, and C Eat.-Legal subCAs issue certs that are ruled by the national Digital Signature Act (DSA), so these certs are used as digital signatures and for code signing. Code Signing certificates are controlled under the DSA.
	
	The A, B, and C subCAs that don't have "Eat.-Legal" in their name issue certs that are not ruled by the national Digital Signature Act (DSA), so these certs cannot be used as digital signatures.
	
	For reference,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

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.	The equivalent of two existing externally-operated subordinate CAs will be created under this root. They are currently under the Class B root which is already included in NSS. Both of these sub-CAs only issue certificates to their own employees. 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 employees of the bank. • This sub-CA does not issue SSL or code signing certificates. • Controlled through CPS, and contract between NetLock and MKB. • See https://bug480966.bugzilla.mozilla.org/attachment.cgi?id=367900 for details of this sub-CA. • MKB is a commercial bank in Hungary, who is operating an external service unit for issuing non-qualified employee signer and encryption certificates. MNB (National Bank of Hungary). • This sub-CA issues signer and encryption certificates for employees of the bank. • This sub-CA does not issue SSL or code signing certificates. • Controlled through configuration of issuing server, CPS, and contract between NetLock and MNB. • See https://bug480966.bugzilla.mozilla.org/attachment.cgi?id=367899 for details of this sub-CA. • MNB (National Bank of Hungary) is the National Bank of Hungary, who is operating an external service unit for issuing non-qualified employee signer and encryption certificates. They are not allowed to create their own sub-CAs. This is controlled through by PATHLEN=0 and by configuration of issuing server. Audits are performed annually by NetLock and by the governmental agency NHH (National Communications Agency).
cross-signing	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: DV, OV, and/or EV	OV • CPS Section 3.2.2, Authentication of Organization Identity • CPS Section 3.2.3, Authentication of Individual Identity • CPS Section 4.2.2: NetLock verifies the identity of organizations as described in the table • 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 EV As per Comment #8, Not requesting EV-enablement at current time.
CP/CPS	Qualified certificate CPS (actual version) in English: https://bugzilla.mozilla.org/attachment.cgi?id=364923 OV, IV verification practice for qualified certificates 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 OV, IV verification practice for non-qualified certificates (not just for signing and time stamping purpose, but for other certifications too) Non-qualified certificate CRL and OCSP profile definitions https://bugzilla.mozilla.org/attachment.cgi?id=366794 Certificate Issuance Practice Statement, valid part https://bugzilla.mozilla.org/attachment.cgi?id=366795 Domain validation practice for non-qualified certificates This is a small still valid part of the 2003-02-25 dated Certificate issuance practice statement. Because the verifications are over defined 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.

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. The audit above ended on 2008-05-06 (before this new root was created) The information below is dated 2009-03-31 Cover letter of the rDSP audit in Hungarian: https://bugzilla.mozilla.org/attachment.cgi?id=378081 Appendix 3 of the rDSP Audit Report (2009-03-31) Hungarian: https://bugzilla.mozilla.org/attachment.cgi?id=378082 English Translation: https://bugzilla.mozilla.org/attachment.cgi?id=378711 This appendix states that the new root is generated following the QA CPS, which is previously audited by the NCA. https://bugzilla.mozilla.org/attachment.cgi?id=378687 Official letter of advice published by the Goverment of Hungary The rDSP auditor is registered by the government with the registration number: 29714-3/2007 > From: Szekeres Balázs <Balazs.Szekeres@cert-hungary.hu> > To: "Kathleen Wilson" <kathleen95014@yahoo.com> > Date: Tuesday, May 26, 2009, 11:26 PM > Dear Kathleen Wilson, > Hereby as the auditor of NetLock Ltd. I confirm that the audit statements provided by NetLock Ltd. to you are > authentic and I confirm that the new “NetLock Arany (Class Gold) Főtanúsítvány” certificate authority root is > operated according to the Hungarian Act 35 of 2001 on electronic signature, the Information and Communication > Ministerial decree 3/2005 (III. 18.). These laws orders that Hungarian CAs have to operated according to criteria that > is at least equivalent to ETSI TS 101 456 or ETSI 102 042. > If you have any further question, please do not hesitate to ask. > Kind regards, > Balázs Szekeres > Technical Manager > CERT-Hungary > url: http://www.cert-hungary.hu

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.
    - 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 qualified roots 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.

Flag Problematic Practices (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 new root will be offline, with subordinate CAs.

- Allowing external entities to operate unconstrained subordinate CAs
  - External entities are allowed to operate subordinate CAs, as described above.
  - The current externally-operated sub-CAs are MNB and MKB. Both of these sub-CAs only issue certificates to their own employees.
- 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, 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.
  - 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
  - Downloaded CRLs without error into Firefox. CRL does not have CIDP extension, and they are not and not will be partitioned.

Verify Audits

(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.
  - Corresponded via email with the rDSP auditor, to confirm the updated audit info.
- 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 reports.