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.)	The 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?)	The NetLock Ltd. is the first qualified Certificate Authority in Hungary, and 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	Status / Notes
Certificate Name	NetLock Arany (Class Gold) Főtanúsítvány	COMPLETE
Cert summary / comments		To Do I see four existing built-in Netlock CAs. Which of them is this new root the rollover for?
The root CA certificate URL Download into FireFox and verify	https://bugzilla.mozilla.org/attachment.cgi?id=365241	COMPLETE
SHA-1 fingerprint.	06:08:3f:59:3f:15:a1:04:a0:69:a4:6b:a9:03:d0:06:b7:97:09:91	COMPLETE
Valid from	2008-12-11	COMPLETE
Valid to	2028-12-06	COMPLETE

Cert Version	3	COMPLETE
Modulus length	2048	COMPLETE
CRL • URL • update frequency for end-entity certificates	Not yet available. CPS section 4.10.1: Validity of the lists is at most twenty-four (24) hours.	When do you expect the CRL to be available?
OCSP (if applicable) • OCSP Responder URL • Max time until OCSP responders updated to reflect end-entity revocation http://www.cabforum.org/EV_Certificate_Guidelines_V11.pdf Section 26(b): "If the CA provides revocation information via an Online Certificate Status Protocol (OCSP) service, it MUST update that service at least every four days. OCSP responses from this service MUST have a maximum expiration time of ten days."	Not yet available.	Not yet available.
List or description of subordinate CAs operated by the CA organization associated with the root CA. (For example, this might include subordinate CAs created to issue different classes or types of end entity certificates: Class 1 vs. class 2 certificates, qualified vs. non-qualified certificates, EV certificates vs. non-EV certificates, SSL certificates vs. email certificates, and so on.)	*1.1.1.* Summary of CAs signed by this root. *Note: This is a plan after the rollover.* 1.1.1.1. Subordinate operated by the CA: The redesigned equivalent of existing roots will be created under this root.	Please provide CA hierarchy information for the existing root(s) that this root will replace.

For internally-operated subordinate CAs the key is to confirm that their operation is addressed by the relevant CPS, and that any audit covers them as well as the root.		
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. (For example, contractual arrangements should require third-party subordinates to operate in accordance with some CPS/CP. Technical arrangements might include name constraints, not allowing them to create their own subordinates, etc.) The extent and nature of contractual and technical controls exercised over subordinate CAs, including: a) Whether or not subordinate CAs are constrained to issue certificates only within certain domains. *[We need a technical description of how this is typically controlled.]* b) Whether or not subordinate CAs can create their own subordinates. *[We need a technical description of how this is typically controlled.]*	1.1.1.2. Subordinate operated by third parties: The equivalent of existing roots will be created under this root. 1.1.1.2.1. MKB (Hungarian Trade Bank) 1.1.1.2.2. MNB (National Bank of Hungary) 1.1.2. Technical controls exercised over subordinate CAs: 1.1.2.1. Certificates issued by subordinates: 1.1.2.1.1. MKB collaborator signer certificate collaborator encryption certificate Controlled trough: - configuration of issuing server, - CPS, - contract between CA and third party. 1.1.2.1.2. MNB collaborator signer certificate, collaborator encryption certificate, partner signer certificate, partner encryption certificate, server certificate (only for internal server authentication) Contorolled trough: - configuration of issuing server, - CPS, - contract between CA and third party. 1.1.2.2. Subordinates options to create subordinates: - They can't create subordinates, controlled trough by PATHLEN - configuration of issuing server.	In regards to subordinate CAs that are/will-be operated by third parties, do MKB and MNB issue certs within their banks or to their customers for use with their services, or other? Please see: https://wiki.mozilla.org/CA:SubordinateCA_checklist

The extent and nature of audits performed against subordinate CAs, including: a) Whether or not subordinate CAs are included within the scope of any audit(s) done against the root CA. b)Whether or not subordinate CAs are subject to third-party audits independent of any audit(s) done against the root CA. c) The frequency at which any audit(s) for subordinate CAs are done.	1.1.3. Audits of subordinate CAs: 1.1.3.1. CA audits of subordinates: Together with the external audits. 1.1.3.2. Third party audits: Made by the govermental agency NHH (National Communications Agency). 1.1.3.3. Frequency of audits: Yearly.	
List any other root CAs that have issued cross-signing certificates for this root CA	None	COMPLETE
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing	I did not find reference to SSL or verification of ownership of the domain name in the CPS. Also did not find reference to Code Signing in the CPS. Is your request to only enable the Email trust bit? Or are you also requesting to enable the Websites (SSL/TLS) and Code Signing trust bits? If you are requestion to enable the Websites and Code Signing trust bits, please provide the location of the documentation that satisfies section 7 of http://www.mozilla.org/projects/security/certs/policy/
If SSL certificates are issued within the hierarchy rooted at this root CA certificate: • Whether or not the domain name referenced in the	OV CPS: • Section 3.2.2, Authentication of Organization Identity • Section 3.2.3, Authentication of Individual Identity	COMPLETE

certificate is verified to be owned/controlled by the certificate subscriber. (This is commonly referred to as a DV certificate.) • 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. (This is commonly referred to as an OV certificate.) • Whether verification of the certificate subscriber conforms to the Extended Validation Certificate Guidelines issued by the CAB Forum. (This is commonly referred to as an EV certificate.)	• 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	
If EV certificates are issued within the hierarchy rooted at this root, the EV policy OID(s) associated with those EV certificates.	EV certificate issuing is planned.	I did not find reference to Extended Validation Criteria in the CPS. Also I do not see evidence of a WebTrust EV audit. Please refer to http://www.cabforum.org/EV_Certificate_Guidelines_V11.pdf Shall we postpone the request to EV-enable this new root?
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).	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.	COMPLETE

• 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 example.		
CP/CPS • Certificate Policy URL • Certificate Practice Statement(s) (CPS) URL (English or available in English translation)	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	Please review the potentially problematic practices listed at http://wiki.mozilla.org/CA:Problematic_Practices. and provide further information if any of these are relevant.
AUDIT: The published document(s) relating to independent audit(s) of the root CA and any CAs within the hierarchy rooted at the root. (For example, for WebTrust for CAs audits this would be the "audit report and management assertions" document available from the webtrust.org site or elsewhere.)	NHH (National Communication Agency, Hungary) audits from their webpage http://webold.nhh.hu/esign/szolgReszlet/init.do?tipus=mi&azon=12201521-2-41 (the website of the agency is under redesign, so that the cause, why the URL contains the "webold" word.) 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 From CPS:The Practice Statement was compiled on the basis of the standard of RFC 3647 [12] according to the recommendations of the Ministry of Informatics and Communication on Public Administration Policies [19]. As to its content, the Practice Statement meets the specifications and recommendations of Act [1], Directive 2/2002. (IV.26) of the Minister of Prime Minister's Office on the security requirements for the services related to qualified digital signatures and the service providers [2] (hereinafter: Directive [2]), and Decree 3/2005. (III. 18.) of the Ministry of Informatics and Communication on the detailed	Please see sections 8, 9, and 10 of http://www.mozilla.org/projects/security/certs/policy/ We need a publishable statement or letter from an auditor (who meets the policy requirements) that states that they have reviewed the practices as outlined in the CP/CPS for these roots, and that the CA does indeed follow these practices and meets the requirements of one of: • ETSI TS 101 456 • ETSI TS 102 042 • WebTrust Principles and Criteria for Certification Authorities Note that this can be a letter/statement that is posted into

	requirements for the services related to qualified digital signatures and the service providers [3] (hereinafter: Decree [3]) and utilizes the recommendations of standards ETSI TS 101 456 [9], ETSI 102 042 [21], as well as X.509 [14].	bugzilla, and then I will need to do an independent verification of the authenticity of the document by contacting the auditor directly. For EV-enablement, will also need a WebTrust EV audit.

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.
    - Could not find.
- 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
- Verify identity info in code signing certs is that of subscriber
    - No mention of code signing in the CPS.
- 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
(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 OV.
- Delegation of Domain / Email validation to third parties
    - ?

- Issuing end entity certificates directly from roots
  - No, will issue via subordinate CAs.
- Allowing external entities to operate unconstrained subordinate CAs
  - External entities are allowed to operate subordinate CAs, as described above.
- Distributing generated private keys in PKCS#12 files
  - 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
  - ?
- OCSP Responses signed by a certificate under a different root
  - ?
- CRL with critical CIDP Extension
  - ?

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.
  - Audit report / Auditor Statement not found.
- For EV CA's, verify current WebTrust EV Audit done.
  - WebTrust EV audit report not found.
- Review Audit to flag any issues noted in the report