Bugzilla ID: 510506
Bugzilla Summary: Add Microsec e-Szigno Root CA 2009 certificate

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.

General Information	Data
CA Name	Microsec Ltd.
Website URL (English version)	http://www.e-szigno.hu/?lap=english
Organizational type.	private
Primary market / customer base.	Microsec Ltd. is a private corporation, primarily operating in Hungary, providing services for the Hungarian general public. Microsec was founded in 1984, it is owned by six Hungarian individuals. Microsec is the IT service provider of the Hungarian Ministry of Justice, and has been developing software for the Ministry and for firm registry courts since 1990. The company started its PKI services in 2002, and became registered as a CA issuing qualified certificates in 2005. We have been providing qualified electronic archiving services since 2007.

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

Info Needed	Data
Certificate Name	Microsec e-Szigno Root CA 2009
Cert summary / comments	This is a new, SHA256, version of the Microsec ShA1 root that is already included in NSS. The new root has a new DN and a new key. Microsec plans to operate the two roots simultaneously for some years, and the old one shall be phased out afterwards. Under the new root, Microsec issues certificates with an OCSP service usable for the general public.
The root CA certificate URL	http://www.e-szigno.hu/rootca2009.crt
SHA-1 fingerprint.	a6:5c:b4:73:3d:94:a5:c8:65:a8:64:64:7c:2c:01:27:2c:89:b1:43
Valid from	2009-06-16
Valid to	2029-12-30
Cert Version	3
Modulus length / key length	2048
Test website	https://pca.e-szigno.hu/
CRL	http://crl.e-szigno.hu/a3ca2009.crl NextUpdate: 25 hours
OCSP	http://a3ocsp2009.e-szigno.hu
CA Hierarchy	Subordinate CAs are created to issue different classes/types of end-entity certificates. These are shown at: http://srv.e-szigno.hu/menu/index.php?lap=english_ca_hierarchy#rootca2009

SubCAs operated by 3rd parties	There are no subordinate CAs operated by third parties.
cross-signing	None
Requested Trust Bits	Websites Email Code
If SSL certificates are issued within the hierarchy rooted at this root CA certificate: DV, OV, and/or EV	OV
EV policy OID(s)	Not EV
CP/CPS	CPS V2.0: http://www.e-szigno.hu/docs/szsz--hsz--altalanos--v2.0.pdf Although the above document is in Hungarian, we have previously submitted an English translation of v1.6 of this CPS, it is available here: http://www.e-szigno.hu/docs/szsz--hsz--altalanos--v1.6--EN.doc The new root and the new hierarchy are the main difference between v2.0 and v1.6. Our CPs and CPSs can be downloaded from here: http://srv.e-szigno.hu/menu/index.php?lap=english_dokszab
AUDIT	Audit Criteria: ETSI TS 101 456 and ETSI TS 102 042 Auditor: Hungarian Government National Communications Authority Auditor Website: http://www.nhh.hu/ Auditor Statement: http://srv.e-szigno.hu/menu/docs/NhhSupervision2008.pdf (2008.08.19) Found on web: http://www.nhh.hu/dokumentum.php?cid=9634 Directorate of Informatics Regulation Dr Nóra SYLVESTER (Ms) sylvester.nora@nhh.hu This auditor has been previously verified. Before approval, will need new audit which includes this root.

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

- Verify domain check for SSL
    - For SSL certificates, Microsec verifies the Subscriber Organization and verifies that the address or domain to be indicated within the certificate of the server is actually held by the Subject, or whether the Subject is in possession of an authorization according to which it has the right to request an SSL certificate for the given address or domain. Domain names are verified using the online registry for appropriate domains, e.g. http://www.domain.hu for the .hu top level domains. If the subscriber is not the registered owner of the domain, Microsec requests an official letter from the owner confirming that the subscriber is allowed to request the certificate.
    - CPS v2.0 p40 (Google Translated): Server SSL Certificates issued to (web server certificates), the Service before issuing the certificate, verify that the server's certificate address or domain is actually owned by the subject, or whether the subject has any mandate that the address of the holder or
      domain, SSL certificate 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.
    - When the requested certificate contains an email address, Microsec verifies that the email address is that of the certificate Subject. Email addresses are verified by sending an email to that address, and the contents of this email are needed at registration.
    - CPS v2.0 p40 (Google Translated): If the subject is e-mail address of the certificate requires the Service Provider Before issuing the certificate, the certificate will verify the e-mail address. Be satisfied that indeed the existing e-mail address and check that the e-mail really address the subject e-mail address.
- Verify identity info in code signing certs is that of subscriber
    - Certificates serving the purpose of signing of computer programs (code signing) and Web server certificates are only issued by Microsec according to certificate class III. The identity of the Subject and the Represented Organization, as well as whether the private key belonging to the public key within the certificate are verified accordingly prior to the issuing of the certificate.
    - CPS v2.0 p40 (Google Translated): Computer programs, signing (so-called code signing) certificate and Web server certificate to the Service solely III. class certification issue, Accordingly, check the certificate before the issuance of the subject and the represented Organization's identity, and that going public key of the certificate magánkulcs the subject held by it.

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

- Long-lived DV certificates
    - We issue certificates for 2 years, and if the Subject requests the renewal of the certificate (with a procedure similar to the first registration) we renew the certificate for the same keypair for another 2 years. Any further certificates are issued for another keypair.
    - This is regulated in Section 6.3.2. of our CPS at http://srv.e-szigno.hu/menu/docs/szsz--hsz--altalanos.pdf This says that the overall validity of all certificates issued to a given keypair cannot be more than 4 years. Theoretically we could issue certificates for 4 years, but we would prefer not to do so. Our DV certificates are also OV.
- Wildcard DV SSL certificates
    - We do issue wildcard DV certificates. We do not have regulations specific to wildcard certificates. Our DV certificates are OV too.

- Delegation of Domain / Email validation to third parties
  - ?
- Issuing end entity certificates directly from roots
  - Not applicable, we do not issue end entity certificates with our root.
- Allowing external entities to operate unconstrained subordinate CAs
  - Not applicable. No sub-CAs operated by 3rd parties under this root.
- Distributing generated private keys in PKCS#12 files
  - ?
- Certificates referencing hostnames or private IP addresses
  - ?
- OCSP Responses signed by a certificate under a different root
  - No. Test website works with OCSP enforced in Firefox.
- CRL with critical CIDP Extension
  - No. CRL imports without error into Firefox.
- Generic names for CAs
  - Root name is not generic