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.
CA's are also encouraged to review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices.

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.
CA Contact Information	CA Email Alias: info@e-szigno.hu CA Phone Number: 36-1-5054444 Title / Department: e-Szignó CA

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_02.crt
SHA-1 fingerprint	89:DF:74:FE:5C:F4:0F:4A:80:F9:E3:37:7D:54:DA:91:E1:01:31:8E
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	CRL issued by root: http://crl.e-szigno.hu/rootca2009.crl Microsec issues CRLs every 24 hours. Next Update is 25 hours. CRL issued by the intermediate CA that issued the certificate for the test website: http://crl.e-szigno.hu/a3ca2009.crl

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: DV, OV, and/or EV	OV
EV policy OID(s)	Not EV
CP/CPS	CPS V2.0 (Hungarian): http://www.e-szigno.hu/docs/szsz--hsz--altalanos--v2.0.pdf CPS V1.6 (English): 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. CP and CPS documents download: 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) New Audit Statement: http://srv.e-szigno.hu/menu/docs/NhhSupervision2009.pdf (2009.10.13) NHH has Microsec listed as both a Qualified and Non-Qualified Registered provider: http://webold.nhh.hu/esign/szolgParams/main.do NHH org chart: http://www.nhh.hu/dokumentum.php?cid=9634 Directorate of Informatics Regulation 2008 auditor: Dr Nóra SYLVESTER (Ms) sylvester.nora@nhh.hu 2009 auditor: Dr. Adam Szilveszter szilveszter.adam@nhh.hu
Organization Identity Verification	From CPS v1.6 EN (note: Service Provider = Microsec) 4.2. Submission and Processing of the Certificate Application New end-user certificates belonging to certification class III or complying with public administration certification policies may be applied for at the customer care center of the Service Provider or at any one of the external registration authorities. The Subject must appear in person for receiving the private key belonging to the certificate. If it is not the Subject appearing before the Service Provider, but the registration staff contacts the Subject, this is in all cases treated as equivalent by the Service Provider. Steps of the application process are as follows: • The Subscriber gathers information regarding the certification policies and certificate types supported by the Service Provider, as well as the conditions of using the service. It may do so using the Web site of the Service Provider or at the customer care center.

	• The Subscriber enters into a service contract with the Service Provider, which specifies the Subjects that are eligible for being indicated on certificates issued within the framework of the contract. • The Subscriber specifies which Subject is authorized to request a certificate according to which certification policy. • The Subject also gathers information regarding the certificate types of the Service Provider, as well as the conditions of using the service. It may do so using the Web site of the Service Provider or at the customer care center. • The Subject indicates to the Service Provider that it is seeking a certificate, submits its data to the customer care center of the Service Provider, and authorizes the Service Provider to manage its data for the purpose of issuing the certificate. • The Service Provider verifies the information specified, with special regards to those that must also be indicated within the certificate. • Should the Subject request a certificate containing an e-mail address, the Service Provider verifies the e-mail address to be indicated within the certificate prior to its issuance. It convinces itself whether the e-mail address actually exists, and verifies whether the e-mail address is the actual e-mail address of the Subject. • In the case of SSL certificates issued for servers (Web server certificates), prior to the issuing of the certificate, the Service Provider verifies whether 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. • Certificates serving the purpose of signing of computer programs (so-called code signing) and Web server certificates are only issued by the Service Provider 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. • The Service Provider compares its data to authentic public databases (for example, the address records or company records). Wherever this is feasible is the case of the specific database, the Service Provider performs data comparison electronically. • In the case of organizational certificates, the Service Provider also requests proof issued by the Represented Organization regarding the fact that the Subject has the right to be indicated within the certificate of the Represented Organization – in the roles indicated. If such proof was not issued directly by the Represented Organization, the Service Provider provides notice to the Represented Organization regarding the fact that it had received such proof. • The Service Provider complies with its information obligation in such a manner so that it makes an information publication available to the Subject. The Subject has an opportunity to study the publication and for consultation. The contents of the publication and the certification application form can also be found on the Web site of the Service Provider, so that these can be viewed in advance. • During registration, the Subject must appear in person before the registration staff of the Service Provider or an external registration organization belonging to it. The registration staff identifies the Subject as described in Section 3.2.3. • A solution which is in all cases equivalent with the first step is when the Service Provider (or its external registration organization) visits the Subject, and performs personal identification at a location specified by the Subject, in line with the security rules of the Service Provider. • The Service Provider identifies the Represented Organization as described in Section 3.2.2.

	• The Service Provider determines the unique name of the Subject, and within the framework of this, assigned a globally unique ID (OID) to the Subject. This is performed as described in Section 3.1.1. • The Service Provider archives the contracts, the certification application, and all proof submitted by the Subject or the Represented Organization. • Prior to these steps, applicants may also refer to their certification applications verbally. They also have the opportunity to study the public documents of the service onsite, moreover they can also receive verbal briefing in connection with the service. • During registration, the Subject provides its own signature as proof that the data specified on the certificate request form is correct, and that its certificate was valid at the point in time of registration. The registration staff of the Service Provider (or external registration organization) uses its signature to prove that the image on the ID of the Subject corresponds to the facial characteristics of the Subject, and that the signature within the ID corresponds to the signature of the Subject. • If the identity of the Subject or its relationship with the Represented Organization cannot be determined beyond all doubt, or any data indicated on the certificate application form is incorrect, the application process is put on hold. At this time, the client has the opportunity to correct the data specified as well as to deliver missing proof. • The Service Provider enters all of the information used to prove the identity of the Subject and the Represented Organization, including the registration number of the documentation used as proof and any potential restrictions connected to its validity.
Domain Name Ownership / Control	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.
Email Address Ownership / Control	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.
Identity of Code Signing 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.
Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices • Long-lived DV certificates o SSL certs are OV o 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. o 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 o SSL certs are OV • Delegation of Domain / Email validation to third parties o Comment #2: We do not delegate domain or e-mail validation (or any operation related to registration) to third parties. If we shall do so in the future, there shall be a contractual agreement between Microsec and the RA. The RA shall adhere to our CP/CPS, and Microsec shall be liable for the activities of the RA. • Issuing end entity certificates directly from roots o Not applicable, we do not issue end entity certificates with our root. • Allowing external entities to operate unconstrained subordinate CAs o Not applicable. No sub-CAs operated by 3rd parties under this root. • Distributing generated private keys in PKCS#12 files o Comment #2: If we generate the private key, it is distributed with a smart card. In case of webserver certificates, we do not generate private keys, we receive PKCS#10 requests only. • Certificates referencing hostnames or private IP addresses o Comment #2: Public addresses are referenced in our certificates only. • OCSP Responses signed by a certificate under a different root o No. Test website works with OCSP enforced in Firefox. • CRL with critical CIDP Extension o No. CRL imports without error into Firefox. • Generic names for CAs o Root name is not generic