Bugzilla ID: 370505
Bugzilla Summary: Add Microsec Ltd root CA 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
Website URL (English version)	http://www.e-szigno.hu/ http://www.e-szigno.hu/index_en.html
Organizational type. (E.g., whether the CA is operated by a private or public corporation, government agency, academic institution or consortium, NGO, etc.)	private
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?)	Microsec Ltd. is a Hungarian certificate authority. 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	Status / Not
Certificate Name	Microsec e-Szigno Root CA	COMPLETE
Cert summary / comments		
The root CA certificate URL Download into FireFox and verify	http://www.e-szigno.hu/RootCA.crt	COMPLET
SHA-1 fingerprint.	23:88:C9:D3:71:CC:9E:96:3D:FF:7D:3C:A7:CE:fC:D6:25:EC:19:0D	COMPLET
Valid from	2005-04-06	COMPLET

Valid to	2017-04-06	COMPLET
Cert Version	3	COMPLET
Modulus length / key length	2048	COMPLET
CRL • URL • update frequency for end-entity certificates	URI: http://www.e-szigno.hu/RootCA.crl Comment #29: A page containing links to our CRLs is available here: http://srv.e-szigno.hu/menu/index.php?lap=english_crl Comment #10: Our CAs issuing end-user certificates issue a CRL every day (i.e. in every 24 hours).	COMPLET
OCSP (if applicable) • OCSP Responder URL • Max time until OCSP responders updated to reflect end-entity revocation EV Guidelines section 26(a): "OCSP responses from this service MUST have a maximum expiration time of ten days."	None for this root Comment #10: As we have a separate OCSP root, you need to install the root certificate of e-Szigno OCSP CA to use our OCSP service. OCSP: URI: https://rca.e-szigno.hu/ocsp	COMPLETI
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.) 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.	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	COMPLETI
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	None shown in the hierarchy diagram. http://srv.e-szigno.hu/menu/index.php?lap=english_ca_hierarchy Comment #32:	COMPLETI

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.)	• Currently there are no external entities who operate CAs subordinated to us. • Section 1.3.2 of our CPS at http://srv.e-szigno.hu/menu/docs/szsz--hsz--altalanos.pdf allows us to have some in the future, and describes some general guidelines: o There needs to be a contract between us and the subordinated CA that regulates the conditions of subordination. o We are responsible for the activities of any subordinated CA. o The subordinated CA may issue certificates for the community defined in the contract. o The subordinated CA must publish its CP, and operate accordingly. We audit their activity. o We revoke the certificate of the subordinated CA if the subordinated CA does not operate according to its own CP or if we learn that its key was compromised. o The subordinated CA may not issue certificates that are to be used in context of the Hungarian public administration. • Section 1.3.2 of our CPS that are used for certificates suitable for creating electronic signatures defines additional criteria: o We need to notify our supervisory authority, NHH if we issue a CA certificate. o The subordinated CA must become a CA registered by NHH. (And thus must undergo the same audit and must fulfill the same criteria that we fulfill.)	
List any other root CAs that have issued cross-signing certificates for this root CA	None shown in hierarchy diagram.	COMPLET
Requested Trust Bits One or more of: • Websites (SSL/TLS) • Email (S/MIME) • Code (Code Signing)	Websites Email Code	COMPLET
If SSL certificates are issued within the hierarchy rooted at this root CA certificate: • Whether or not the domain name referenced in the 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	DV, OV Comment #32: Yes, we verify both the domain name and the organization before we issue the certificate.	COMPLET

to be that associated with the certificate subscriber. (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.)		
If EV certificates are issued within the hierarchy rooted at this root, the EV policy OID(s) associated with those EV certificates.	N/A	N/A
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 example.	For instance: https://www.magyarorszag.hu/ and our own website https://www.e-szigno.hu/	COMPLETE
CP/CPS • Certificate Policy URL • Certificate Practice Statement(s) (CPS) URL (English or available in English translation)	Comment #32: Bullets 7, 8 and 9 on page 37 have been added, they can be translated as follows: * In case the Subjects requests a certificate containing an e-mail address, the CA verifies this e-mail address before the certificate is issued. The CA verifies that the address is indeed an existing e-mail address, and also verifies that the e-mail address is indeed the e-mail address of the Subject. * In case of SSL certificates for servers (webserver certificates), before issuing the certificate the CA verifies that the address or domain to appear in the server certificate is indeed owned by the Subject, or the Subject possesses a written statement that entitles the Subject for requesting an SSL certificate for the given address or domain. * Certificates suitable for signing computer programs (known as code signing certificates) are issued as Class 3 only, this means the CA verifies using a face-to-face registration both the identity of the Subject and/or represented organization and the fact that the public key to appear in the certificate is controlled by the Subject. Comment #24:	COMPLET

	We have updated our CPS-s as we promised in our commitment letter. The required update is in Section 4.2 of the documents. For example, our CPS at http://srv.e-szigno.hu/menu/docs/szsz--hsz--altalanos.pdf contains the required statements on page 37, bullets 7, 8 and 9. The rest of our CPS-s do not deal with webserver and code signing certificates, they contain the statement on the verification of e-mail addresses only. Comment #10: Our CP/CPS is available in Hungarian only. All of our CPs and CPSs follow the structure of RFC 3647. We had to demonstrate it during our audit, so we prepared a table for this purpose. We have decided not upload it to this bugzilla, but we uploaded it to our web server, and we would like to remove it after this procedure is over if possible. This table is temporarily available at: https://srv.e-szigno.hu/MicrosecCPs--RFC3647.pdf Comment #29: Our CPs and CPSs can be downloaded from here: http://srv.e-szigno.hu/menu/index.php?lap=english_dokszab (unfortunately, the documents are still in Hungarian only)	
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.)	Hungarian Government National Communications Authority: http://www.nhh.hu/ Auditor Statement: http://srv.e-szigno.hu/menu/docs/NhhCertification.pdf https://bugzilla.mozilla.org/attachment.cgi?id=255220 Found on web: http://www.nhh.hu/dokumentum.php?cid=9634 Directorate of Informatics Regulation Dr Nóra SYLVESTER (Ms) sylvester.nora@nhh.hu Also see http://www.nhh.hu/dokumentum.php?cid=11653&mid=1032	COMPLETE

	Email sent on 6/23/2008 to verify audit report. Response Received 8/7/2008: As you asked, I surely can verify: that document was signed by me, and it is authentic. The National Communication Authority supervises every year the Microsec ltd. as qualified certificate issuer. The Microsec Ltd. is figured on the list of e-Signatures register : http://webold.nhh.hu/esign/szolgReszlet/init.do?tipus=mi&azon=10589605-2-41 You can check it and see other documents about the market of hungarian electronic signatures at our website: http://www.nhh.hu/index.php?id=hir&cid=960&mid=718&lang=en Nóra Sylvester director Directorate of Informatics Regulation National Communication Authority	

Review CPS sections dealing with subscriber verification (COMPLETE)

- Verify domain check for SSL
    - "In case of SSL certificates for servers (webserver certificates), before issuing the certificate the CA verifies that the address or domain to appear in the server certificate is indeed owned by the Subject, or the Subject possesses a written statement that entitles the Subject for requesting an SSL certificate for the given address or domain."
- 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.
    - "In case the Subjects requests a certificate containing an e-mail address, the CA verifies this e-mail address before the certificate is issued. The CA verifies that the address is indeed an existing e-mail address, and also verifies that the e-mail address is indeed the e-mail address of the Subject."
- Verify identity info in code signing certs is that of subscriber
    - "Certificates suitable for signing computer programs (known as code signing certificates) are issued as Class 3 only, this means the CA verifies using a face-to-face registration both the identity of the Subject and/or represented organization and the fact that the public key to appear in the certificate is controlled by the Subject."
- Make sure it's clear which checks are done for which context (cert usage)

Flag Problematic Practices (COMPLETE – info is from comment #32)

- Long-Lived Domain-Validated SSL certs

    - 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 certs
    - We do issue wildcard DV certificates. We do not have regulations specific to wildcard certificates. Our DV certificates are OV too.
- Issuing end entity certs directly from root rather than using an offline root and issuing certs through a subordinate CA
    - Not applicable, we do not issue end entity certificates with our root. We have a figure on our website illustrating which CA issues what kind of certificates in our hierarchy: http://srv.e-szigno.hu/menu/index.php?lap=english_ca_hierarchy This is regulated in Section 1.3.1 of our CPSs.
- Allowing external entities to operate subordinate CAs
    - Currently there are no external entities who operate CAs subordinated to us.
    - Section 1.3.2 of our CPS at http://srv.e-szigno.hu/menu/docs/szsz--hsz--altalanos.pdf allows us to have some in the future, and describes some general guidelines:
        - There needs to be a contract between us and the subordinated CA that regulates the conditions of subordination.
        - We are responsible for the activities of any subordinated CA.
        - The subordinated CA may issue certificates for the community defined in the contract.
        - The subordinated CA must publish its CP, and operate accordingly. We audit their activity.
        - We revoke the certificate of the subordinated CA if the subordinated CA does not operate according to its own CP or if we learn that its key was compromised.
        - The subordinated CA may not issue certificates that are to be used in context of the Hungarian public administration.
    - Section 1.3.2 of our CPS that are used for certificates suitable for creating electronic signatures defines additional criteria:
        - We need to notify our supervisory authority, NHH if we issue a CA certificate.
        - The subordinated CA must become a CA registered by NHH. (And thus must undergo the same audit and must fulfill the same criteria that we fulfill.)

Verify Audits

- Validate contact info in report, call to verify that they did indeed issue this report.
    - COMPLETE
- For EV CA's, verify current WebTrust EV Audit done.
    - Not EV
- Review Audit to flag any issues noted in the report

- No issues noted